Code of Ethics

As a law enforcement officer, my fundamental duty is to serve society, to safeguard lives and property, to protect the innocent against deception, the weak against oppression or intimidation, and the peaceful against violence or disorder, and to respect the constitutional rights of all people to liberty, equality, and justice.

I will keep my private life unsullied as an example to all; maintain courageous calm in the face of danger, scorn, or ridicule; develop self-restraint; and be constantly mindful to the welfare of others. Honest in thought and deed in both my personal and official life, I will be exemplary in obeying the laws of the land and the regulations of my department. Whatever I see or hear of a confidential nature or what is confided to me in my official capacity will be kept secret unless revelation is necessary in the performance of my duty.

I will never act officiously or permit personal feelings, prejudices, animosities, or friendships to influence my decisions. With no compromise for crime and with relentless prosecution of criminals. I will enforce the law courteously and appropriately without fear of favor, malice, or ill will, never employing unnecessary force or violence and never accepting gratuities.

I recognize the badge of my office as a symbol of public faith and accept it as a public trust to be held so long as I am true to the ethics of the police service. I will constantly strive to achieve these objectives and ideals, dedicating myself before God to my chosen profession—law enforcement.
<table>
<thead>
<tr>
<th>Directive #</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Use of Force</td>
</tr>
<tr>
<td>2</td>
<td>Active Shooters Preparedness</td>
</tr>
<tr>
<td>3</td>
<td>Reassignment Policy</td>
</tr>
<tr>
<td>4</td>
<td>Uniform and Equipment</td>
</tr>
<tr>
<td>5</td>
<td>Telephone Procedures</td>
</tr>
<tr>
<td>6</td>
<td>Memorandums</td>
</tr>
<tr>
<td>7</td>
<td>Handling of Prisoners</td>
</tr>
<tr>
<td>8</td>
<td>Mobile Prisoner Transport</td>
</tr>
<tr>
<td>9</td>
<td>Detention Unit Security</td>
</tr>
<tr>
<td>10</td>
<td>Court Security</td>
</tr>
<tr>
<td>11</td>
<td>Prisoner-Defendant Security</td>
</tr>
<tr>
<td>12</td>
<td>Judicial Threats-Witness Protection</td>
</tr>
<tr>
<td>13</td>
<td>High Risk Trials</td>
</tr>
<tr>
<td>14</td>
<td>Prisoner Escapes</td>
</tr>
<tr>
<td>15</td>
<td>Funeral Details</td>
</tr>
<tr>
<td>16</td>
<td>Hospital and Transportation Detail</td>
</tr>
<tr>
<td>17</td>
<td>Transportation of Prisoner(s) Via Aircraft</td>
</tr>
<tr>
<td>18</td>
<td>Warrant Unit Procedures</td>
</tr>
<tr>
<td>19</td>
<td>Use of Law Enforcement Vehicles</td>
</tr>
<tr>
<td>20</td>
<td>Notification to the Sheriff</td>
</tr>
<tr>
<td>21</td>
<td>Civil Enforcement Glossary</td>
</tr>
<tr>
<td>22</td>
<td>Outside Employment</td>
</tr>
<tr>
<td>23</td>
<td>Sick Leave Policy</td>
</tr>
<tr>
<td>24</td>
<td>Real Estate Sales &amp; Enforcement</td>
</tr>
<tr>
<td>DIRECTIVE #</td>
<td>SUBJECT</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>25</td>
<td>ENFORCEMENT OF WARRANTS &amp; SUBPOENAS</td>
</tr>
<tr>
<td>26</td>
<td>ENFORCEMENT OF INJUNCTIONS TRO</td>
</tr>
<tr>
<td>27</td>
<td>ENFORCEMENT OF STAY ORDERS</td>
</tr>
<tr>
<td>28</td>
<td>LEGAL DOCUMENTS (TIME-BOUND) ENFORCEMENT</td>
</tr>
<tr>
<td>29</td>
<td>CRIME SCENES</td>
</tr>
<tr>
<td>30</td>
<td>COMMENDATIONS</td>
</tr>
<tr>
<td>31</td>
<td>WELLNESS UNIT</td>
</tr>
<tr>
<td>32</td>
<td>ARMORY WEAPONS, AMMO, &amp; FIREARMS</td>
</tr>
<tr>
<td>33</td>
<td>TRAINING AND SELECTION</td>
</tr>
<tr>
<td>34</td>
<td>TRAUMATIC INCIDENTS</td>
</tr>
<tr>
<td>35</td>
<td>PEER SUPPORT PROGRAM</td>
</tr>
<tr>
<td>36</td>
<td>INFORMATION TECHNOLOGY OPERATIONS POLICY</td>
</tr>
<tr>
<td>37</td>
<td>HARASSMENT-FREE WORKPLACES</td>
</tr>
<tr>
<td>38</td>
<td>CRISIS COMMUNICATIONS</td>
</tr>
<tr>
<td>39</td>
<td>ROLL CALL AND INSPECTIONS</td>
</tr>
<tr>
<td>40</td>
<td>PERSONNEL STATUS AND ELECTRONIC COMPLIANCE</td>
</tr>
<tr>
<td>41</td>
<td>DOMESTIC VIOLENCE AND DEPUTIES/STAFF</td>
</tr>
<tr>
<td>42</td>
<td>OFFICE RELATIONSHIPS</td>
</tr>
<tr>
<td>43</td>
<td>OFF DUTY LAW ENFORCEMENT ACTIONS</td>
</tr>
<tr>
<td>44</td>
<td>PA COMMISSION ON CRIME &amp; DELINQUENCY EDUCATION &amp; TRAINING PROGRAM</td>
</tr>
<tr>
<td>45</td>
<td>REMOVAL OF PERSONS FROM CITY MEETINGS</td>
</tr>
<tr>
<td>46</td>
<td>SOCIAL MEDIA</td>
</tr>
<tr>
<td>47</td>
<td>SUBSTANCE ABUSE SCREENINGS</td>
</tr>
<tr>
<td>48</td>
<td>CYBER SECURITY INCIDENT RESPONSE PLANS</td>
</tr>
<tr>
<td>49</td>
<td>CIVILIAN GRIEVANCES</td>
</tr>
<tr>
<td>50</td>
<td>RELEASE OF PUBLIC INFORMATION</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>DIRECTIVE #</th>
<th>SUBJECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>51</td>
<td>REQUESTS FROM ELECTED OFFICIALS</td>
</tr>
<tr>
<td>52</td>
<td>PHILADELPHIA SHERIFF'S OFFICE-INJURY/EXPOSURE POLICY</td>
</tr>
<tr>
<td>53</td>
<td>CHAIN OF COMMAND</td>
</tr>
<tr>
<td>54</td>
<td>WRITTEN DIRECTIVES</td>
</tr>
<tr>
<td>55</td>
<td>DISCIPLINARY PROCEDURES</td>
</tr>
<tr>
<td>56</td>
<td>CODE OF CONDUCT</td>
</tr>
</tbody>
</table>
Office of the Sheriff
City and County of Philadelphia, Pennsylvania
Land Title Building
100 S. Broad Street, 5th Floor
Philadelphia, PA 19110

February 24, 2021

The purpose of the Directive: Policies and Procedures is to explain to all members of the organization, directives, policies, and procedures of the Philadelphia Office of the Sheriff (PSO). Directives, as used interchangeably within this document with policies and procedures, are broadly stated principles and values intended to guide members in the performance of their duties in conformity with department objectives. Directives are methods of performing law enforcement activities to achieve our objectives. The directives, policies, and procedures may be general or specific in nature, but it is the responsibility of each member of this organization to be familiar with the contents of this document, and any Standard Operating Procedures (SOP) Manual utilized by your division or unit.

These directives do not and cannot address every situation a member may encounter while in the performance of his/her law enforcement duties. If a member encounters a situation that is not covered by directive, policy, procedure, or training, the member will be expected to exercise sound judgment and act in accordance with the Office of the Sheriff Mission Statement, Core Values, and Guiding Principles. There may be times when it is necessary for a member to take action that may not fully comply with a stated directive, policy, or procedure. In such situations, the member will be required to justify the deviation from stated policy or procedure and those actions will be subject to strict review.

Adherence to these directives, policies, and procedures will ensure the Office of the Sheriff Mission, Vision, Core Values and Guiding Principles. In doing so, it reinforces our collective commitment as professional law enforcement providers, to provide professional services, fairly and ethically at all times, to all people, in order to proactively address crime, reduce inequity and graft in Sheriff Sales, and to promote procedural justice in the community.

Rochelle Bilal
Sheriff of Philadelphia, Pennsylvania

Disclaimer: "This Manual is for internal use only and does not enlarge an employee's civil liability in any way. The Manual should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of any directive within this manual, if proven, can only be used for internal purposes in accordance with the laws governing employee discipline."
VISION, MISSION, CORE VALUES, & GUIDING PRINCIPLES

The Philadelphia Office of the Sheriff is a dynamic, progressive, and professional organization dedicated to maintaining community partnerships which promote a high quality of life for the diverse population in the City and County of Philadelphia. This Office is committed to treating all people with dignity, fairness, and respect, protecting their rights, and providing equal protection under the law as a law enforcement agency in the Commonwealth of Pennsylvania.

VISION: The Office of the City and County of Philadelphia Sheriff, a law enforcement agency committed to excellence, will become a national benchmark in the professional delivery of sheriff related services under our purview; we strive for high performance, equally high customer satisfaction, and accept and integrate innovative ideas to remain dynamic and flexible.

MISSION: The Office of the City and County of Philadelphia Sheriff is committed to service, procedural justice, and the sanctity of human life. Our duties encompass protecting the lives, property, and rights of all people within a framework of service, uncompromising integrity, fiscal responsibility, professionalism, vigilance, and bias free conduct.

CORE VALUES
1. Service above self
2. Integrity without compromise
3. Professionalism on/off the job
4. Vigilance in safeguarding our stakeholders

GUIDING PRINCIPLES
1. Professionalism and Organizational Excellence
2. Community Engagement and Partnerships
3. Operational Improvements/Performance Metrics
4. Technology Development and Infrastructure Expansion
1. PURPOSE:

A. The purpose of this Directive is to establish a policy on the Use of Force by members of the Philadelphia Sheriff’s Office, which is line with the Sheriff’s Office’s high regard for human life and the dignity of the human being. It is intended to express the Office’s commitment to holding every human being as valuable and to uphold the sanctity every human life. The overall principle conveyed by this Directive is that every Deputy Sheriff has a sacred duty to preserve human life.

B. Although deputies are to have a deep affinity for the preservation of human life, times will arise in a deputy’s career when she/he will have to use force to quell a violation of the law or to protect the life and persons of others. In these instances, the amount of force used shall be based upon two standards. One is “objective reasonableness.” Objective reasonableness is the legal standard for the use of force. It dictates that a deputy’s actions should be viewed within the context of what amount of force would a reasonable deputy on the scene of an incident use the in that circumstance. A deputy’s actions are considered lawful if she/he believed the actions were legal according to an obviously instituted law and that information possessed by the deputy at the time of the action would justify the deputy’s actions. The totality of a deputy’s actions must meet the standard of objective reasonableness. This means that the deputies are accountable for their decisions which led up to the situation, where the use of force is required. Deputies shall be mindful that if their pre-use of force conduct created the situation in which force became necessary, they could still be liable for their actions. This legal concept is called “officer-created jeopardy”.

While situations involving threats to public safety are unpredictable, deputies should begin developing flexible plans before they arrive on the scene of the incident. In this way, they can utilize a wide range of response options, including de-escalating a situation without resorting to excessive force. These means acquiring as much information as possible before arriving on scene of an incident. One of the tools available to deputies as they respond to incidents, where force may have to be used is
the “use of force continuum”. The use of force continuum allows the deputy responding to an incident to assess the scene of incident and to select which level of force is appropriate for the situation. The key factor in the amount of force to be exerted by the deputy shall be the suspect’s resistance to the public safety demands, the law and deputy commands, respectively.

Use of Force Continuum:

It shall be noted that the level of force, required in any incident, is depended on upon the subject’s resistance to a deputy’s lawful commands and the subject’s conformance to the law and public safety demands. It is not necessary to go through a lower level on the Use of Force Continuum, if it is obvious to the deputy that the incident requires a higher level of force for resolution. A deputy’s conduct shall never be the reason why the force level is raised. We want to de-escalate and not instigate conflicts.

1. **Deputy Presence:** Deputy Presence is used when a subject is compliant. It is the best deterrent of crime and to defuse potential violent situations. Deputy’s appearance shall be clean, neat, and very professional looking, to project the right message of competency and alertness. The deputy’s attitude shall be professional, respectful, nonthreatening, and confident. The most important aspect of deputy presence is situational awareness. Being cognizant of her/his surroundings, allows the deputy to best gauge what level of force is needed to resolve a situation or when the threat level of a suspect has risen to a higher level. There are three segments of situational awareness. The first is based upon the actions of the subject. The second is founded upon the deputies’ response to the subject’s action. The last is rooted in the deputy’s perception of risk posed by subject’s actions. Be mindful that your response to the subject’s actions and your perception of risk, both must be reasonable.

2. **Verbalization:** When dealing with a compliant subject, a Deputy shall issue calm nonthreatening commands. When speaking, deputies shall display confidence and firmness, not arrogance. Deputies shall not be degrading or condescending when speaking to or commanding a civilian. A deputy’s speech may be intensified or used in short commands in more serious situations.

3. **Empty-Hand Techniques:** When dealing with a passive resistive subject, a deputy shall employ empty-hand techniques. Passive resistance is when a subject is not threatening a deputy but is failing to comply with a deputy’s lawful commands. Empty-hand techniques include grabs, holds, “take down moves” and joint locks. These are considered soft tactics. Once compliance has been effectuated, the deputy shall refrain from the use of all force.

4. **Less-Than-Lethal Methods:** For actively resistant subjects, deputies are to employ techniques designed to quell the active resistance to their lawful commands. Active resistance is defined as resistance, where a subject physically resists a
deputy’s commands and control, and which puts the deputy, the subject, or another person at risk for bodily injury. Less-than-lethal methods are comprised of fists, kicks, batons, OC spray and stun gun. Once compliance has been affected, the deputy shall refrain from the use of any and all force.

(5) **Lethal Force:** Lethal force is the force of last resort. Lethal force can only be used when a deputy has reasonable belief that a subject’s actions present a significant risk to the life of the deputy or other persons or poses a threat of serious bodily harm to the deputy or other persons.

C. Unreasonable acts of force are illegal, detrimental to relations between law enforcement and the public and carry civil liabilities for our Office. Deputies, who commit acts of unreasonable force, may be subject to civil and criminal sanctions. For this reason, it is vital for deputies to be able to not only justify their use of force based upon objective reasonableness but be able to articulate it. Bear in mind all a deputy’s actions must be reasonable throughout the incident. Any instigation of hostilities on the part of the deputy could lead to legal liability. Remember a good intention is not a substitute for reasonableness.

D. All members of the Sheriff’s Office shall exhibit a reverence and respect for the dignity of all persons and the sanctity of human life in all contacts with the public. This includes the unfortunate reality of the use of force. The authority of the Sheriff’s Office is derived from the public and therefore makes all Sheriff’s Office members **public servants**. This reality vanquishes the idea of deputies as warriors, as we are not at war with our fellow citizens. We are **Guardians**, whose primary duty is to protect the rights, lives, and persons of our fellow citizens as they are processed through our legal system. When the need to use force arises, it will only be exercised to prevent the loss of life, prevent injury and to preserve the peace.

E. As stated earlier in this directive, a deputy will have to use force sometime in her/his career as not every potential violent confrontation can be de-escalated. However, deputies do have the ability to affect the direction and outcome of many situations based upon their training, decision-making skills, and/or the tactics they choose to employ before they use another level of force. At each level of force, a deputy shall when safely possibly utilize de-escalation techniques.

F. **Definitions:**

1. **Force** is defined as the compulsion or restraint upon or against a person for the purpose of:

   a. Compelling a person to comply with a deputy’s lawful instructions; or

   b. Overcoming resistance by a suspect during and arrest or detention; or
c. Defending any person or yourself from an aggressive action by a suspect or another, to prevent injury or death.

Note: After any use of force, where injuries are sustained by all parties involved in the use of force incident, deputies are to when circumstances permit, render medical care consistent with her/his training. Medical care may include providing basic first aid, requesting emergency services, and /or arranging for transportation to a medical facility. Deputies shall inquire from all arrestees, who were subject to a use of force, if injuries were sustained by them during the incident.

2. Excessive control/force results when the use of force is greater than that justified by the violator’s level of resistance at the time the force was used. It should be noted that when physically resistive subject ceases her/his resistance and complies with deputy commands, the use of force must be terminated and reduced to deputy presence and custody/detention of the subject. Legally, excessive force is defined as force used by government officials that exceeds the minimum amount of force needed to diffuse an incident or to protect themselves or others for harm. Prohibitions against excessive force are rooted in the Fourth Amendment’s reasonable search and seizure requirement and the Eighth Amendment’s ban on cruel and unusual punishment.

3. Deadly force is any force that is reasonably likely to cause death or serious injury. Deadly force can also result from a less-lethal force option being improperly applied. The Supreme Court Case, Tennessee Vs. Garner rests necessary deadly force on two (2) pillars: the first is to prevent escape and the second is that the deputy has probable cause to believe that the subject poses a significant threat of death or injury to the her/himself or others. These two factors must co-exist in an incident, for the use of deadly force to be justified. Deputies shall when circumstances permit and when it is reasonably practical, identify themselves as law enforcement officers and give a clear verbal warning of their intent to use deadly force.

NOTE: Deputies must render medical care consistent with their training to subjects, who survive deadly force incidents. Medical care may include providing basic first aid, requesting medical services and/or arranging for transportation to a medical facility.

4. De-escalation: De-escalation techniques and tactics are actions taken by deputies, when safe and feasible without compromising law enforcement priorities, that seek to minimize the likelihood of the need to use additional force during an incident and increase the likelihood of voluntary compliance on the part of the subject.
a. If circumstances allow deputies shall conduct a threat assessment so as not to precipitate an unnecessary, unreasonable, or disproportionate amount of force by placing themselves or others in undue jeopardy. In the threat assessment consider if the subject’s non-compliance is deliberate or due to an inability to comply, such as:

Medical conditions
Mental impairment
Developmental disability
Physical limitation
Language barrier
Drug interaction
Behavior crisis
Fear and anxiety

b. Team approaches are encouraged in matters of de-escalation. Deputy training, skill level, number of deputies and whether any deputy has established a rapport with the subject should be considered when choosing tactics and techniques of de-escalation. When using a team approach to de-escalation, every deputy’s action must be in harmony with the overall strategy of de-escalation.

c. Selection of de-escalation options shall be guided by the totality of the circumstances of the incident and be made with the goal of obtaining voluntary compliance from the subject; considerations shall include:

(1) Communication—is used to gain voluntary compliance from a subject. Communication includes verbal persuasion; explaining to the subject why non-compliance is not good for her/him. Warnings made in a calm and respectful manner can be used to obtain compliance. It should be noted that threats are not a de-escalation tactic. Warnings are statements explaining what the results of her/his actions could be, while threats are statement of what the deputies are going to do to the subject if compliance is not obtained. One of the most effect tools in de-escalation is the LEED technique:

LISTEN-Allow people to tell their side of the story, give them voice and let them vent.

EXPLAIN-What you’re doing, what they can do and what’s going to happen.
EQUITY- Tell them why you are taking action. The must be fair and free from bias and show their input was taken into consideration.

DIGNITY-Act with dignity and leave them with their dignity.

(2) Time-When safe and feasible under the totality of the circumstances, deputies shall attempt to slow down or stabilize the situation, so that more time, options, and resources are available for resolution. Scenes stabilization supports transitioning a situation from dynamic to static by limiting access to unsecured areas, preventing mobility, and preventing the involvement of uninvolved community members. Deputies should avoid or minimize physical confrontation unless physical confrontation is necessary to maintain law enforcement priorities. This tactic gives the deputy time to request extra resources such medical staff or less-than-lethal certified deputies to the scene.

(3) Distance-Deputies shall maximize tactical advantage by maintaining a distance which allows for law enforcement functions to be performed but also gives deputies enough space for greater reaction time.

(4) Shielding-Deputies shall use cover and concealment to gain a tactical advantage over a hostile subject. This means placing a barrier between the hostile subject and deputies.

5. **Objectively reasonable force** is the legal standard for the use of force in the United States. It is defined as the determination from the perspective of a reasonable deputy on the scene of an incident that the decision to use force and the amount of force used are appropriate when evaluating the situation in light of the circumstances and what was known to the deputy at the time of the incident.

6. **Officer-created jeopardy** is defined as situations where law enforcement officers needlessly place themselves in danger by committing unforced tactical errors that makes them vulnerable and thus in a position where they must use lethal force to protect themselves. Deputies must aware that more and more the courts are looking to see if law enforcement pre-use of force conduct is reasonable.
7. **Control** for the purposes of this directive is defined as the actual physical control of a subject that allows for the completion of a lawful arrest/detention.

8. **Choke Hold** is a physical maneuver or technique that restricts an individual’s ability to breathe for the purpose of incapacitation. **It shall be duly noted that the use of choke holds is strictly forbidden for Sheriff’s Office personnel.**

9. **Hogtie restraint** are any form or variation of restraint by which the wrists are handcuffed behind the back, the ankles are bound together, and the bound wrists and ankles are then tied together. **It shall be duly noted that the use of hogtie restraints is strictly forbidden for Sheriff’s Office personnel.**

10. **Distraction Techniques** are acts used to divert or redirect a subject’s focus away from resistive or dangerous behavior in order to assist the deputy in gaining control of individual. Distraction techniques **may include a controlled palm strike, pressure points or leverage techniques targeting a specific area that has the greatest likelihood of effectiveness and is not intended to cause serious bodily injury.** If a distraction technique proves ineffective, a different distraction technique or force option should be considered. **A closed fist, or punch, is not a distraction strike.**

2. **POLICY:**

   A. Having the authority to use force in public service is an awesome responsibility and it places a tremendous burden on each deputy to understand that every human life is valuable, and every human being has a right to dignity. The preservation and the betterment of life should guide every action made by deputies in the Philadelphia Sheriff’s Office. Since the protection of life is our core motivation, it imperative that deputies only use the minimum amount of force needed to prevent the loss of life and the breaking of the peace.

   B. The use of force guidelines is intended for internal Office use and have not been developed for application in any civil or criminal proceeding, nor are they intended to create a higher legal standard of safety or care with respect to third parties. A violation of this directive will be grounds for administrative discipline only, while a violation of the law may be the basis for civil or criminal penalties imposed by a court of law.
C. The provisions of this order are applicable to all sworn deputies acting in their capacity as law enforcement deputies.

D. If the subject is to be detained, arrested, or searched and it is reasonable to do so, deputies shall make their intentions to the subject that is to be arrested, detained, or searched. When practical deputies will identify themselves as a law enforcement deputy before using force.

E. All sworn personnel at every rank have the duty to intervene when observing another duty using force that is beyond that which is objectively reasonable under the circumstances.

F. Deputy Involved Critical Incidents shall define in this directive as any of the following:

1. A Philadelphia Sheriff’s Office employee or any person in and around any court facility sustains serious bodily injury.

2. An activity (even if someone is impersonating to be) an employee of the Philadelphia Sheriff’s Office results in death or injury to a deputy or a citizen.

3. Any incident that requires Joint Emergency Operations Center (JEOC) activation.

4. Any significant event that results in mass media coverage and requires a Philadelphia Sheriff’s Office command presence, such as mass arrest, vigil disturbance or Sheriff’s Office personnel involved homicide.

5. Act of terrorism, active shooter, hostage, or barricaded person situations in and around court facilities.

6. Any situation which the Sheriff declares to be an emergency and Executive Staff command presence is required.

These incidents shall be responded to by the Unit Commander, who has the responsibility for the area in which the incident happened or who supervises the personnel involved. The Unit Commander shall conduct a preliminary investigation, however the first supervisor on the scene shall:

a. Ensure that all apparently injured deputies, employees and citizens are provided with emergency medical attention.
If a deputy has been injured, the Unit Commander:

(1) Shall always assign an uninjured deputy to remain with and accompany the deputy.

(2) Assign a deputy to give in-person notification to the injured duty’s family. The assigned deputy shall remain with the family as to service its immediate needs and shall be the liaison between the Sheriff’s Office and the family.

(3) Ensure that the injured deputy’s weapon and duty equipment are secured.

(4) Take care to preserve the integrity of any physical evidence (e.g. blood, fingerprints) on the deputy or the deputy’s equipment or clothing until authorized investigators or lab personnel arrive.

(5) Ensure that if a suspect, employee and/or general citizen is injured, a deputy be assigned to and remain with each injured party and accompany them to a medical treatment facility. It should be noted that at least two (2) shall be assigned to the suspect.

(6) Make proper notifications to the Chief Deputy, Internal Affairs Division, and the Public Information Officer.

(7) Attempt to gain a brief overview of the situation from involved deputies. This should only include a general representation of events in the incident to address public safety concerns, to discover the scope of the incident and scene and to brief the Internal Affairs Division, when they arrive on scene.

b. Once notified of a Deputy Involved Critical Incident (DICl), the Commander of the Philadelphia Sheriff’s Office Internal Affairs Division shall:

(1) Conduct an administrative investigation of the incident, beginning with debriefing of the affected Unit Commander and supervisors subordinate to that Commander, in order to ensure no violations of Sheriff’s Office policy were committed by
Office personnel. Ensure that all personnel interviewed receive Garrity Warnings, unionized personnel shall be notified of their right to union representation and that the physical and psychological needs of all incident involved staff have been addressed prior to being interviewed.

(2) Ensure that the Philadelphia Sheriff’s Chief Deputy and Office Public Information Officer (PIO) are kept abreast of the details of the investigation and notified immediately of major findings.

(3) Shall issue a final report of findings to the Sheriff’s and submit a statement of charges to the Undersheriff for staff who have violated Office policy.

3. **PROCEDURE:**

A. **DE-ESCALATION:** As stated in section one (1) of this directive, not every potential violent confrontation can be de-escalated non-violently. However, deputies by using training, good decision-making skills and the proper tactics can greatly influence the outcomes of these encounters. It shall be the duty of each deputy to bear in mind that the primary reason why we engage in these confrontations are to preserve human life and to preserve the peace.

1. The overall goal of this policy is to promote thoughtful resolutions to situations and to reduce the likelihood of harm to all persons involved. De-escalation is reviewed and evaluated under the totality of the circumstances present at the time of the incident or known by the deputy at the time of the incident.

2. A deputy shall only implement de-escalation techniques when it is safe, feasible and doesn’t compromise law enforcement priorities to do so.

   a. In circumstances that meet the above criterion, deputies shall conduct a threat assessment. Considerations shall be made according to the entirety of Part 1, section F, sub-section 4 of this directive.

B. **Use of Force-Scene Responsibilities**

1. Initially involved/responding units shall:
a. Take necessary and proper law enforcement action to ensure the scene is stabilized and all threats to deputy safety and the public are resolved.

b. Provide immediate first aid to all injured parties, when it is reasonable to do so and request appropriate to do so.

c. Ensure the crime scene is properly identified, preserved, and protected. If needed, request additional personnel to assist. The crime scene perimeter should be large enough provide safety, security, and confidentiality.

d. Identify, protect, and secure all evidence at the scene. Do not move anything unless it’s absolutely necessary.

e. If inside the perimeter of the identified crime scene, exit as soon as possible.

f. If charge of the crime scene log, or if guarding the inner perimeter, make sure that anyone attempting to enter the crime scene perimeter has a legitimate investigative purpose for being there. Maintain your assignment until properly relieved by the appropriate Philadelphia Police Department (PPD) Units and then assume control of the inactive scene.

g. If feasible, prior to PPD’s arrival canvass the area for witnesses. Obtain positive identification of all individuals in the immediate area that may have been involved or a witness to the incident. Ensure witnesses are cared for and kept separated for one another.

2. The initial Philadelphia Sheriff’s Office supervisor on scene shall:

a. Assume field command of the situation, ensuring all activities are carried out in accordance with Philadelphia Sheriff’s Office procedures. Determine the category within the incident falls, notifies the Unit Commander and remains in command until relieved by the Unit Commander or by an equivalently of higher ranked PPD supervisor.

b. Evaluate and assess the medical and/or psychological needs of the involved employees and ensure employees remain at the scene unless conditions dictate otherwise.

c. Ensure the crime scene is properly secured and protected with tightly controlled access until the arrival of the Unit Commander or investigative personnel.
d. Ensure that a crime scene log has been created. Only persons entering the actual crime scene should be documented on the crime scene log. Personnel who arrive on scene but do not enter the crime scene should not be entered in the crime scene log. The log will be maintained until a PPD officer relieves the deputy of the crime scene responsibilities. A copy of the log shall then be turned over to the PPD and retained by the responding Philadelphia Sheriff's Office supervisor to ensure it is transferred to the Unit Commander and/or Philadelphia Sheriff's Office Internal Affairs investigator.

e. Establish a preliminary command post outside of the scene.

f. If necessary, establish a specific area for the media to meet with a designated spokesperson. Ensure the media is kept outside of the perimeter and way from the preliminary command post and involved employees. Any statements should be coordinated with the PPD investigator and the Philadelphia Sheriff's Office and PPD public relations personnel.

g. Gather sufficient to provide an overview to the investigative personnel, keeping in mind that in-depth interviews of involved and/or witness employees in critical law enforcement incidents shall only be conducted the Philadelphia Sheriff's Office investigator.

h. Shall evaluate the crime scene needs. Pursuant to their responsibilities maintaining crimes scenes, the supervisor shall redeploy any employees present at the scene and uninvolved as participants, witnesses, or crime scene security to their regular duties.

i. Shall assist the Unit Commander to coordinate with assigned investigative personnel providing whatever assistance is essential to the successful operation of the investigation.

3. The affected Unit Commander shall:

   a. Ensure that all the provisions of the above sub-section are followed.
   b. Follow the provision set forth in Part 2, section F of this directive.

C. Force Options: All use of force actions by deputies are predicated upon the actions of the subject(s). Deputies can only use the amount of force necessary to make an arrest or a detention or to protect her/him or others. Force can only be applied for as
long as it takes to subdue the suspect. Once deputies have gained objectively reasonable control of a subject, all use of force shall terminate. Any force used after that point is excessive. Deadly force shall not be used except as specially provided for in this directive. The Office’s training material on the use of force is hereby incorporated as if fully set forth herein.

1. During a lawful contact a subject may be:

   a. **Compliant:** A person contacted by a deputy who acknowledges direction or lawful orders given and offers no passive/active, aggressive, or aggravated aggressive resistance.

   b. **Non-Compliant:**

      1. Passive Non-Compliance: The subject is not complying with the deputy’s commands but is not using physical force to defy the deputy. The person may lock her/his arms, stop moving, go limp or tighten her/his body. Reasonable force options to passive non-compliance include low level force options.

      2. Active Resistance: The subject is physically resisting the deputy’s commands but is not doing so to harm the deputy. The subject in this case is physically trying to prevent the deputy’s control of her/him. Subjects in this category use from of resistance like pulling away from the deputy or breaking the deputy’s grip. Reasonable force options to be used against active resisting subjects include low level force options and intermediate force options. It is strongly discouraged to closed fist strikes against grounded persons as this increases the risk of injury to the deputy and the subject.

      3. Aggressive Resistance: The subject is intent on harming the deputy, her/himself, or other person(s) and to prevent the deputy from placing her/him into custody and taking control. The aggression from aggressive resistance may manifest itself as threats to injure the deputy, her/himself or others, punching, kicking or other actions which present a legitimate risk of injury to the deputy or others. Reasonable force options for aggressive resistance are limited to low level force option to intermediate. It should be noted the longer that aggressive resister incident lasts the more likely the situation will evolve into an aggravated aggressive resistance.
4. Aggravated Aggressive Resistance: The subject’s actions are likely to result in death or serious bodily harm to deputy, themselves, or another person(s). These actions include the use of firearms, bladed or blunt weapons and extreme physical force. Any amount of force is reasonable when a deputy is responding to an aggravated aggressive subject. 

   Note: Whenever a deputy applies a use of force option upon a subject which results in an injury or complaint of injury, the deputy will monitor the subject; render first aid to the best of their skill level. And immediately summon medical attention and a supervisor to the scene.

2. In response to the above situations, deputies shall be guided in the use of force as follows:

   a. **Low Level Force**-a level of force or control that is neither likely nor intended to cause injury, i.e., handcuffing a compliant arrestee for transport to/from jail or placing a subject in a prone position on a high-risk pedestrian atop. Low level force includes documenting de-escalation attempts and:

      1) Deputy Presence-Subject recognizes the deputy’s author through a uniformed presence, marked vehicles, badges, sheriff’s markings or logo, deputy sheriff credentials and verbal identification and de-escalation communication. At no time should a deputy become insulting, condescending, or rude to any citizen, regardless to his status as a civilian, subject of investigation or arrestee. If the subject is compliant, the deputy should explain what she/he is doing and what’s going to happen and if possible her/his version of what happened in the incident which made her/him subject to investigation. Excludes physical force.

      2) Verbal Commands-Commands of direction or required compliance such as direction to drop a weapon, to get on the ground stop running, etc. Commands shall be clear, loud enough to be heard and understood, logical and consistent. Throughout the encounter Deputies are to remain professional and refrain from any comments which might exacerbate tensions and cause a higher level of force to be used.

      3) Weaponless Strategies-level 1 – Techniques designed or required to gain compliance through open hand control techniques (such as takedown with no injury or handcuffing).
4) Weaponless Strategies-level-2 – Techniques designed to gain compliance through the use of control device approved of by the Philadelphia Sheriff’s Office such as handcuffs or use of an approved restraint device.

b. Intermediate Force- a level of force that has the potential to cause injury or substantial pain and is greater than low level force.

1) Weaponless Strategies-level 1 – Techniques designed to gain compliance through empty hand control techniques such as strikes, takedowns with injury or pressure points.

2) Weapon Strategies- 2 – Techniques designed to gain compliance using a departmentally approved control techniques device such as impact weapons, chemical agents or conducted electrical weapons (CEW)

c. Deadly Force- a level of force which is likely to produce death or serious bodily injury.

3. Use of Force Restrictions: As it is our oath to support, obey and defend the United States Constitution, members of the Philadelphia Sheriff’s Office shall pay close attention to the mandates of the Constitution’s provisions which guide us in our duties as public servants. At all times, deputies shall recognize the Constitutional prohibitions against illegal searches and seizures and cruel and unusual punishment, uphold the principles freedom of speech and equal protection under the law. Deputies shall understand that the Constitution places restrictions on our conduct as law enforcement officers. Deputies shall be aware that violations of Constitutional prohibitions may not only result in administrative discipline, but also carry criminal and civil penalties. These restrictions, like all written policies, may not cover every situation. Any deviation shall be examined meticulously on a case-by-case basis.

a. Deputies shall not use deadly force in response to a verbal threat of serious bodily harm or death.

b. Deputies shall not fire a weapon as a warning to compel arrest, or to prevent the escape of a prisoner.

c. Deputies shall not fire a weapon from a moving vehicle.

d. Deputies shall not fire a weapon into a moving vehicle or at its occupant(s), unless the occupant(s) is using deadly force against the deputy or another present, by means or than a vehicle.
e. Deputies shall not place themselves in the path of a moving vehicle in a manner which may lead to the use of deadly force. If a confrontation with a moving vehicle does occur, deputies shall move out of the path of the vehicle.

f. Deputies shall not fire into buildings where suspects are obscured there-in. The only exception to this rule is in instances where there is no doubt of the suspect’s location, and then only a deadly assault or an intended deadly assault is being directed against deputy or others.

g. A deputy shall not discharge her/his weapon at animals, except to protect her/himself or another person from physical injury and if there is no other reasonable means to eliminate the threat.

h. Deputies are prohibited from using choke holds and other types of neck-restraining techniques, except when protecting themselves or others against an imminent threat of serious injury and/or dead.

i. Deputies are prohibited from using a hogtie restraint.

j. Deputies having a firearm drawn or exhibited shall secure the weapon before engaging a suspect in a different weapon strategy (conducted electrical weapon, baton or oleoresin capsicum or pepper spray) a weaponless strategy, or transitioning to a form of control which requires physical contact.

(1) Tactical Units, when carrying out duties in accordance with approved procedures stated in their unit Standard Operations Procedure (SOP) and in accordance with the Unit advanced training, may prove an exception when exigent circumstances place the deputy at significant tactical disadvantage, or risk of serious bodily injury or death.

k. Deputies shall not use a firearm as a club, or to strike any person.

4. Control Devices: Deputies and supervisors shall carry only departmental approved conducted electrical weapons (CEW), chemical agents, and expandable batons after completing the prescribed course of instruction from the Sheriff's Office Training Division.

5. A list of approved chemical agents and batons/accessories shall be maintained by the Training Unit Deputy Chief, and all list will be maintained at the Training Unit. All procedures and guidelines for control devices, including reporting regulations, shall apply to both uniformed and plain-clothes deputies. Control devices shall only be used in situations authorized by Directive, the Training Unit and the CEW Training guidelines.
6. Expandable Baton

a. The expandable baton shall only be carried by deputies who have qualified for use of said device.

b. All expandable batons must be obtained at the deputy’s expense and will not be replaced by the Sheriff’s Office in the event of loss or damage.

c. End caps that are used for retention purposes to prevent the baton from slipping from the deputy’s hand are authorized. This excludes any end caps that has pointed or sharpened protrusions or window breaking feature which may cause additional injury while being used during close mode strikes.

7. Chemical Agents

a. Deputies trained and authorized by the Philadelphia Sheriff to carry and utilize chemical agents and delivery systems (OC Spray) issued by the Sheriff’s Office shall do so within the standards of Sheriff’s Office training standards.

b. Deputies shall not use chemical agents on a subject who is displaying passive non-compliance or who does not demonstrate an overt intention to use violence or force against themselves, deputies, or another person.

c. Once deputies have exposed a subject to a chemical agent, deputies shall seek medical assistance, if the subject has the following conditions:

   (1) Pre-existing medical condition, including pregnancy
   (2) Appear to be under the influence of a narcotic or controlled substance.
   (3) Appear non-responsive, ill or have difficulty breathing.
   (4) When circumstances allow, deputies are encouraged to immediately begin decontamination by rinsing the exposed areas with clean water.

d. All issued chemical agents shall be inspected by the Training Unit personnel during annual firearms re-qualifications.

8. Conducted Electrical Weapons (CEW)

a. Only Sheriff’s Office issued CEW’s are authorized to be used by deputies; personally, owned CEW’s are not authorized.

b. Deputies shall only draw or exhibit CEW, when:

   (1) Conducting a Sheriff Office approved spark test to ensure proper operation of CEW.
(2) There is articulatable belief that the use of the CEW is in conformance with Directives, Office Control Tactics Training Manual and CEW Training Guidelines.
(3) Any type of horseplay with the CEW is strictly prohibited.

c. CEW shall be carried in an approved holster on the support (non-dominant) side of the body.
d. CEW demonstrations/presentations are prohibited when conducted by CEW instructors with the approval of the Training Unit Captain.
e. A request shall be made to medical personnel to remove all probes that penetrate the skin, except in exigent circumstances.

(1) Probes that enter sensitive tissue such as head, faces, genitals, necks, or breast shall be removed by medical personnel.

(2) Probes that penetrate the skin are biohazards and shall be disposed using an FDA (Food and Drug Administration) recommended bio-waste container. Deputies who receive a puncture from a used probe shall follow the Office’s exposure procedures as outlined in the Directives.

(3) Latex gloves shall be used when handling the removed probe.

f. Once the CEW has been activated against a subject (drive stun or probes)

(1) Deputies shall request a medical evaluation on-scene (ambulance) or
(2) Request transport to a hospital for evaluation when a subject cycle for more than a cumulative fifteen (15) seconds.

g. Deputies shall consider the physical condition of the subject and the subject’s surroundings which could potentially result in a high-risk danger such as, but not limited to, a fall from a great distance or into the path of moving vehicle when determining whether the CEW is an appropriate option.

h. CEW are prohibited on the following high-risk population unless exigent circumstances exist or to prevent serious bodily injury or death to the subject, the deputy or a third person.

(1) Infirm (frail, weak)
(2) Elderly
(3) Low body-mass index
(4) Pregnant
(5) Juvenile
(6) Person in water (drowning risk)
(7) Handcuffed

i. A supervisor or unit commander shall respond to the scene of every CEW activation, in drive stun or cartridge mode.

j. All use of the CEW as ARC display, in the drive stun mode, and/or in the cartridge mode shall be documented in the offense/incident report which the deputy shall note as a “Use of Force”. Accidental cartridge discharges shall be reported in a memorandum explaining the incident to the deputy’s immediate supervisor where it will be signed and forwarded to the Deputy Chief of the Training Unit.

k. **Drawing the CEW from the holster in preparation of the possibility of use in considered a use of force.**

(1) When completing the administrative Use of Force report involving activation against a suspect, the supervisor will perform a download of the deputy’s CEW firing record. This information will be attached to the report.

(2) The only exceptions to documentation of CEW use are spark testing and official Training Unit classes and demonstrations.

l. All CEW and cartridges shall be inspected at the roll call and by Training Unit personnel during annual firearms/CEW qualification.

m. No repair or alteration shall be performed on the CEW except by approved Training Unit staff. Any malfunction or necessary repair shall be immediately reported to the Deputy Chief of Training for appropriate action.

n. All data stored in CEW is subject to downloading by the Sheriff’s Office.

o. The Training Unit shall maintain a current list of Deputies qualified to carry/use the CEW and a list of Deputies who have been issued CEW equipment.

**D. Use of Deadly Force**

1. The use of deadly force is **authorized only when it is necessary for deputies to protect themselves or others from an immediate threat of death or serious bodily injury.** Justification for the use of deadly force shall be limited to facts known or reasonably perceived by a deputy at the time the incident occurs. Deputies are reminded that if
circumstances permit and it is reasonably practical, they shall identify themselves as law enforcement officers and should give verbal warning of their intent to use deadly force.

2. Regardless of the nature of the crime or justification for the use of deadly force, deputies must always remember their basic responsibility is to protect the public. Therefore, except to preserve life or to prevent serious bodily injury, deputies shall not fire their weapon under circumstances that would subject other deputies, bystanders or hostages to death or possible injury.

3. The use of deadly force is always considered a DICI.

E. Discharges/Use of Firearms

1. A Deputy Sheriff shall not remove her/his firearms from a holster except when a reasonable belief exists that the use of deadly force may be necessary or when the circumstances dictate that a firearm be secured. The display of a firearm is considered a use of force and shall require reporting as such.
2. Deputies shall always use care to ensure the safe handling of firearms and shall always treat a firearm as if it is loaded.
3. A deputy shall not discharge her/his firearm at animals except to protect her/himself or another person from physical injury and if there is no other reasonable means to eliminate the threat.
4. A deputy shall not use a firearm as a club.
5. A deputy is prohibited from firing warning shots.
6. No Deputy shall carry a firearm until she/he had demonstrated proficiency to the Training Unit.
7. No Deputy Sheriff shall be issued a long gun, shotgun or weapon of any type until demonstrating proficiency in the use of the same to the training unit.
8. This includes carrying privately owned “off-duty” firearms. Each off-duty firearm shall be registered with the Firearms Training Unit and must be approved prior to authorization to carry in any capacity.
9. Any Deputy Sheriff who discharge a weapon accidentally or intentionally shall:
   a. Notify a supervisor and the local police department via 9-1-1 (or police radio) as rapidly as the situation permits.
   b. Inform the 1st supervisor on the scene of the location(s) of the crime scene(s) and the general circumstances relative to the preservation and collection of physical evidence. This may require the deputy to conduct a walk-through of the scene with the supervisor.
c. Deputies are prohibited from making statements to press. All inquiries from the media concerning a discharge or use of force shall be forwarded to the deputy’s supervisor and the Sheriff’s Communications Deputy.

d. Deputies will cooperate with the investigation of the incident by providing a statement to Internal Affairs; this provision shall not be construed to prohibit the deputy from speaking to any counselor or union representative regarding the incident while at Internal Affairs, or any time afterwards.

10. If a deputy is outside of the Philadelphia County jurisdiction, the deputy who discharged the firearm shall:

a. Notify supervisor and the local jurisdiction’s police via 9-1-1 as rapidly as the situation permits.

b. Comply with the instructions given by local law enforcement officials.

c. Call the Sheriff Communication Deputy, so that proper notifications can be made.

d. Notify a Sheriff’s Office supervisor who shall make an immediate electronic critical incident notification to members of the Executive Command Staff.

11. Sheriff’s Office Dispatch shall:

a. Ensure that a District Supervisor or local police supervisor is dispatched to the incident scene.

b. Immediately notify a Sheriff’s Office supervisor.

c. Notify the Sheriff and Chief Deputy via telephonic notification.

12. The first Sheriff’s Office Supervisor on the incident scene shall be responsible for the following:

a. Ensure that a local police department supervisor has been notified and responds to the location(s) of occurrence.

b. Determine which deputy(s) fired their weapon(s) by examining magazines/cylinders of the weapon of each deputy present during discharged.

c. Recall to the scene any deputy having left the scene prior to the Sheriff’s Office supervisor’s arrival to inspect their weapon(s).

(1) Glock (semi-automatic) weapon inspection: Instruct the deputy(s) to remove the magazine for inspection and note the number of rounds and take possession of the magazine. Supervisors are not to handle the weapon at any time, only the magazine.
d. Allow involved deputy(s) to retain custody of the firearm absent any exigent circumstances and reload their weapon with a new magazine. This will ensure that the deputy(s) have a fully loaded weapon while being transported to Internal Affairs Division.

e. Ensure that information concerning the location(s) of the crime scene(s) and the general circumstances relative to the preservation and collection of physical evidence is provided by the involved deputies and disseminated to the assigned investigator by remaining at the scene until the arrival of a supervisor.

f. Ensure that the immediate details are entered into the electronic critical incident notification system to be forwarded to the Executive Command Staff.

13. In cases of discharges outside of this jurisdiction Internal Affair Division shall:

a. Notify the local investigative agency, speak to assigned investigator, and direct a Philadelphia Sheriff’s Office Internal Affairs Division Team to the scene of the DICl and/or meet with the assigned investigator.

b. The IAD assigned investigator will respond to any discharge by PSO employees within reasonable driving distance (<3hrs).

c. If permissible, obtain any documents and/or interviews pertaining to the discharge.

F. Reporting Use of Force Incidents

1. All use of force incidents which result injury to any person, involves the use of a physical method of control that includes a strike or the grounding/takedown of a subject, or any display/use of a weapon to control a subject shall be reported and identified as a “Use of Force”. Deputies shall take careful note that any and all omissions of facts related to the use of force shall be deemed falsifications of a Sheriff’s record.

2. Deputies shall report the full details of the use of force in related arrests or offence reports. If no arrest or offense report is to be completed the details shall be reported in an incident report. A separate administrative report will be completed by the supervisor and electronically forwarded through the deputy’s “chain of command” for review.

3. To provide the most accurate Use of Force statistics, a County Suite Use of Force report shall be generated. The report shall contain a space for each suspect’s description (name, DOB, address, PP number, etc.) involved in the use of force.
The report shall also generate a number for each use of force, with following use of force reports receiving the next sequential number.

a. An administrative report is not required for the grounding/takedown or handcuffing of an individual where no injury or other force is applied.

4. All reports which detail a use of force incident shall be completed prior to the end of the deputy’s shift.

5. Supervisors of deputies who utilize force will closely review and provide critiques of all incidents that involve a deputy using strikes on subjects on the ground to ensure the reasonableness is explained and/or guidance is provided regarding tactical considerations when responding to such resistance. This critique shall be memorialized in memorandum, which shall be attached to the deputies’ incident reports.

6. Only after the use of force report has reached the level of the Deputy Chief in charge of training or at the request of the Training Division Captain, shall a Use of Force panel be installed to review a use of force report.

7. The Deputy Chief in charge of the Training Division shall review each use of force report to determine if there is a need for changes in departmental procedures, additional training for the deputy and/or a referral to City of Philadelphia’s Employee Medical psychologist; the deputy’s commanding officer shall take appropriate action based on the recommendation of the Deputy Chief in charge of training. All incident that rise to the level of a Deputy Involved Critical Incidents or meet the criteria to be reviewed by a Use of Force Review Panel, shall be referred to the Sheriff and the Chief Deputy.

8. All use of force reports shall be tracked by the Training Division. The purpose of tracking these reports is for data analysis and to ensure the Training Division has the most current information available as it pertains to the utilization and effectiveness of use of force tactics and to potentially identify trends in criminal tactics. Requests for Training Division evaluation of a specific Use of Force incident shall be directed to the Deputy Chief of the Training Division and must meet the criteria listed below:

   a. Involve a lawful arrest or detention.
   b. Involve a tactical violation or disproportional use of force as defined in the disciplinary guidelines.
c. Not an Incident defined by the Directives as Deputy Involved Critical Incident (DICI).

9. The Internal Affairs Division shall conduct an end of the year use of force audit. A report of the audit results shall be generated for review by the executive staff and published for the public on the Sheriff’s Office website. The Annual Use of Force Report will be due on the 15th of January of every year.

10. It is recognized that exigent circumstances may occur requiring a deputy to use a weapon or device that is outside of current policy. Any use by a deputy of a weapon or device that is not approved by the Sheriff’s Office, shall be reported as Deputy Involved Critical Incident.

G. Investigation of Firearms Discharges

1. The involved deputy shall:
   a. Whether or not the discharge results in death or injury to any person, shall be temporarily assigned to non-public/prisoner contact duties within their unit.
   b. Have their case reviewed within five business days by Internal Affairs Unit and returned to active unless circumstances exist that dictate otherwise.

2. Philadelphia Police Department Homicide Unit:
   a. Investigates all cases involving the discharge of firearms by deputies resulting in or likely to result in the death of a human being. They will be responsible for the preparation of the Investigation Report (75-49), which would be forwarded to Sheriff’s Office Internal Affairs in seven (7) calendar days.

3. The Philadelphia Police department Crime Scene Unit:
   a. Processes the crime scene after conferring with the assigned investigator.

4. The involved deputy’s immediate supervisor shall:
   a. Ensure that Sheriff and Internal Affairs were notified.
   b. Contact the Employee Assistance Unit (EAP), within five (5) business days in order to arrange confidential counseling whenever a deputy has discharged their firearm.
c. Coordinate with the Captain of the Training Unit and assign the involved deputy to mandatory firearms training before their return to duty.
d. Should the Internal Affairs Division, determine that circumstances exist to require the deputy to remain on non-public/prisoner contact duty, then IAD commander shall submit a memorandum to the Sheriff within five (5) business days of the firearms discharge seeking an approval to extend the time of non-public/prisoner contact. If the extension is approved an additional five days (5) shall be granted or more time if the circumstances warrant it.
e. Prepare a separate of supplemental report (entered into CountySuite System) detailing the results of the internal investigation.
f. Upon completion of the supplement report, the Deputy Chief in charge of the Internal Affairs Division will forward a complete investigative report to the employee’s Deputy Chief, the Chief Deputy and the Sheriff via County Suite System.

H. Use of Force Training

1. The Office of the Sheriff Training Manual outlines the appropriate use of force techniques approved for use by all sworn personnel. All Sheriff’s Office Use of Force Trainings shall contain the following:

   a. An explanation of the 4th and 8th Amendment of the U.S. Constitution and the Supreme Court Case Tennessee v. Garner and how they relate to the use of force.
   b. A force continuum or matrix that provides “detailed descriptions of what force is appropriate at various levels of encounters”.
   c. An emphasis on force proportionality, minimization, and de-escalation.
   d. Conflict avoidance tactics.
   e. A requirement that deputies warn before using lethal (and sometimes other) force.
   f. A requirement that deputies exhaust available forms of force short of deadly force before using deadly force.

2. All deputies of the rank of captain and below shall qualify annually in the Office approved expandable baton, CEW and open-hand control training program. Failure to demonstrate qualification standards in practical and written examinations will result in remedial training with certified control tactics instructor, after which a retest shall be given. Failure of the retest shall be considered as neglect of deputy to disqualification from the reserve program for failure to maintain an acceptable level of performance.
3. Requirements for firearms are outlined in the Firearms Qualification directive.
4. It shall be the responsibility of the Training Division Captain to ensure appropriate training is developed and offered annually. The captain also shall ensure that the appropriate documentation of training and certification is entered in each deputy’s training and personnel file.
5. In the event of changes in training regarding the use of force, the Training Division shall notify the Sheriff, Chief Deputy, and Internal Affairs.
6. It shall be the responsibility of all supervisors to ensure their personnel attend the appropriate training and maintain certification.

I. Use of Force Review Panel

1. The Sheriff’s Office through the process of a Use of Force Panel shall at the request of the Sheriff or Sheriff’s designee and at least once per year, convene a Use of Force Review Panel to examine and review all aspects of the use of force related incidents which meet following criteria:

   a. Involved a lawful arrest or detention,
   b. Deemed as unreasonable force as defined by the use of force disciplinary code.
   c. Incidents defined as Deputy Involved Critical Incident (DICl) involving the use of force.

2. The Use of Force Review Panel shall also review Office statistics, policy, and training regarding use of force, as well as work to seek and gain Office-wide feedback where such is appropriate.

3. The focus of the Use of Force Review Panel shall be to protect the sanctity of life, improve deputy safety, enhance professionalism and provide liability protection by evaluating the use of force employed in each incident with emphasis on reasonableness, adherence to Office policy and following best practices. The Use of Force Review Panel shall not be disciplinary, nor shall any disciplinary recommendations be sought or considered from the review board.

4. The composition of the Use of Force Review Panel shall be flexible to ensure an extensive and insightful review is conducted. The members will meet quarterly or as directed by the Chairperson. The members shall (at minimum) consist of:

   a. Use of Force Coordinator: Chairperson
   b. Two (2) Command Staff Representatives at the rank of Captain or above
c. Representatives Training Division Representatives not to exceed two (2) members (selected by the training Division Captain)
d. One (1) Internal Affairs Division Representative
e. One (1) FOP Representative
f. Rank-in-file Deputy Representatives not to exceed three (3) deputies; each deputy assigned must be Sheriff’s Office veterans of at least five years of service and must be under a satisfactory evaluation.
g. Two (2) Representatives from Community Organizations, with focus on legal or law enforcement issues.

5. Members of this panel shall be briefed by the Sheriff in the operational procedures of the board before being given the responsibility of reviewing use of force incident packets or serving as chair.

6. The Use of Force Review Panel shall by majority accord, determine whether the force is reasonable and within the Office policy and current best practices.

7. The chairperson of the panel shall direct the preparation of the conclusion and findings of the board. A formal proposal will be developed through the chairperson and the Training Division Representatives and shall be next forwarded to the Sheriff for suggested education based and/or policy changes before January 31st of each year.

BY ORDER OF:

[Signature]

SHERIFF DATE
DIRECTIVE: #2
SUBJECT: ACTIVE SHOOTER PREPAREDNESS
ISSUE DATE: 03-25-2020
REVISED DATE: 02-24-2021

1. PURPOSE:

A. It is the policy of the Philadelphia Sheriff's Office, based on training, best practices, and the sanctity of human life, to allow initial responding deputies the authority and imbue responsibility to take immediate action to neutralize active threats during incidents that pose an ongoing danger to human lives.

B. Because of the urgency and dynamic nature of an active threat situation, the first responding deputy must assess and quickly assume management responsibility of the scene until relieved by someone of higher authority.

C. Federal, state, and local law enforcement personnel can be an invaluable resource in developing a prevention and preparedness component of an active shooter program. As such, it is in the best interest of this agency and the facilities we serve to build strong partnerships with other those we serve, fellow law enforcement, fire personnel, and EMS to ensure they also know active shooter protocols, the location of available public announcement systems, two-way communications systems, security cameras, and alarm controls.

D. Equally important is information on access to utility controls, medical supplies, and law enforcement equipment. Through on-going training in active shooter response and by providing detailed information to fellow first responders, we facilitate a response that allows for rapid movement during an emergency, to ensure and/or make areas safe, and to tend to people in need.

E. A Philadelphia Police Department Special Weapons and Tactics (SWAT) supervisor, after being briefed by the scene manager, will then assume Tactical Command.

2. DEFINITIONS
A. Definitions

1. Active Threat: An active threat situation is one which an armed person or person(s) have used deadly physical force on other persons and continues to do so while having unrestricted access to additional victims.

2. Contact Person or Team: An initial team of uniformed Deputies/Police Officers, working together, that moves through a building for the sole mission of identifying and neutralizing the active shooter(s).

3. Rescue Team: A second team of uniformed Deputies/PoLice/EMS Officers, working together, that moves through a building to locate and treat/rescue victims.

3. PROCEDURES

A. Uniform Operations

1. Each Office facility shall have an active shooter preparedness plan, which is to be updated every two years, as needed. At a minimum, a plan should comprise the following elements:

   a. Security Assessments
   b. Preparedness
   c. Communication
   d. Incident Plan (i.e., actions to take during an incident)
   e. Training and Exercises
   f. Post Incident Recovery
      i. Employees
      ii. Operations

2. As plans are drafted, reviewed, and updated, The Deputy Chief Uniform Operations will designate a Uniform Operations Captain as the Designated Official or designee in each facility where deputies serve. The Designated Official shall collaborate with the facility management (e.g. President Judge, Council President, etc.), on-site law enforcement agencies (if applicable), and first responder agencies likely to address an active shooter situation.

3. Uniform Operations Captains assigned as Designated Officials shall collaborate with other tenants/agencies in development and maintenance of the plan.

4. The Deputy Chief, Uniform/Tactical Operations shall provide training, materials, and/or awareness discussions to inform employees of active shooter preparedness plans as they are updated.
a. Employees should be aware of the run, hide, fight concept. 
https://www.youtube.com/watch?v=5VcSwejU2D0&feature=emb_title

b. Employees should be informed of the importance of having a personal plan.

c. New employees should be given active shooter preparedness training during the initial onboarding period.

d. In an effort to ensure training of employees in facilities served by the Office of the Sheriff, the Uniform Operations Captain at each facility shall coordinate with facility management and ensure active shooter training is extended to civilian entities in all facilities once per quarter year.

5. The active shooter plan need not be a stand-alone document. The agency/facility security officials and/or Designated Official will determine the best way to incorporate the active shooter plan into existing protocols.

6. As previously noted, the six points above are policy requirements for all facilities covered by the Office of the Philadelphia Sheriff. What follows throughout the rest of this document is a set of best practices meant to assist with the implementation and maintenance of an active shooter plan as mandated by this policy.

B. The first deputy /deputies on the scene will:

1. Immediately assess the situation, acting to neutralize the threat, if possible and if opportune.

2. Establish and assume the preliminary responsibilities of Incident Commander:

3. The first deputy on-scene will inform the Board Supervisor and all responding deputies via Radio of the situation and request a supervisor.

4. The first deputy one scene first will assume command and instruct responding deputies of the best way to approach the active shooter situation, including the suspected location of the shooter(s).

5. Responding supervisors and deputies will switch their handheld radios to Philadelphia Sheriff's Office channel B-11.

6. Upon being notified of an active threat event, the Sheriff Supervisor shall assign a dedicated deputy to handle communication on channel B-11 and Philadelphia Police Radio, A-13 (J-Band).
7. Make the decision to rapidly deploy (18 Pa. C.S. Section 508 "IDOL" (Immediate Defense of Life); and establish and brief a Contact Team and a Rescue Team.

8. There should be at least one (1) deputy remaining outside of the incident location to control the scene and keep Sheriff's Radio informed. The communications deputy/supervisor will assume incident command, and will:

a. Assess and verify conditions and keep Sheriff's Radio informed.
b. Establish communication with Sheriff's Operation and Command Post
c. Notify Sheriff's Radio of the safest ingress/egress routes and designate an on-scene radio officer.
d. Request necessary resources (i.e. SWAT, Bomb Squad, Hostage Negotiators, etc.) and give staging area location.
e. Gather intelligence from persons on the scene.
f. Establish preliminary inner and outer perimeters.
g. Determine access points.
h. Maintain Incident Log.

9. First responder intervention will be based on opportunity. Contact and Rescue Teams will be in the form of two (2) or more uniformed deputies/policemen officers regardless of rank, one of whom will be identified as the "element leader". If a supervisor is not on scene and circumstances warrant immediate intervention, a deputy sheriff may assume the role of "element leader". Team movement will be in a controlled and disciplined tactical action under control and direction of the element leader.

C. Contact Team

1. Absent exigency will have no less than two (2) uniformed deputies/policemen officers, or a combination. Their mission is to locate and neutralize the suspect(s).

a. Form a flexible formation. Prior to entry, all members will acknowledge their role and responsibility in the formation.

b. The Contact Team will:

1. Make contact with the suspect(s).
2. Stop deadly behavior
3. Limit suspect(s) movement.
4. Prevent escape.
5. Relay information to the Command Post.
6. Notify Sheriff's Radio of the location of any victim(s) they discover.
2. After the suspect(s) have been controlled or it has been determined that they are no longer an immediate threat, the contact team will secure the area so the Medical Support can be provided to the injured.

3. Based on conditions and circumstances, the Incident Commander will have the ability to assemble additional contact teams consisting of deputies/police officers as needed for large scale locations or multiple suspects.

D. Rescue Team: Forms to rescue and/or evacuate victims to a safe zone by:

1. Use of the Flexile "T" formation which will consist of four (4) deputies/police officers.

2. Communicate to the Contact Team before entry and update the Command Post.

3. Strong communication is necessary between the Contact Team, Rescue Team, Incident Command, and Supervisor.

4. Based on conditions and circumstances, the Incident Commander will have the ability to assemble additional rescue teams consisting of four (4) deputies/police officers, as needed for large scale locations or multiple victims.

5. The shooter or conspirators may be among the victims. The Rescue Team will remember all safe practices when encountering any victim at the scene. If possible, all victims will be patted down for weapons and officer safety.

6. Responding deputies should use extreme caution and be aware of primary and possible secondary explosive devices intended to injury first responders as they arrive to an active shooter incident.

E. Deployment of Rapid Assessment Medical Services:

1. This deployment shall include the addition of Philadelphia Fire Department Medics.

2. Must be approved by the Fire department command and the Sheriff's Office command.

3. Be part of the Rescue Team only.

4. Use of the diamond formation which will consist of five (5) deputies/police officers.
IV. INCIDENT COMMAND: SUPERVISORY RESPONSIBILITIES

A. Supervisory responsibilities: The first supervisor on the scene will relieve the first deputy on the scene as Incident Commander.

1. The Incident Commander regardless of rank shall:

   a. Assess and verify conditions and keep Sheriff's Radio informed.
   b. Establish communication with Sheriff Operations and Command Post
   c. Notify Sheriff's Radio of the safest ingress/egress routes and designate an on-scene radio officer.
   d. Request necessary resources (i.e. SWAT, K-9, Bomb Squad, Hostage Negotiators, etc.) and give staging area location.
   e. Gather intelligence from persons on the scene.
   f. Establish inner and outer zones.
   g. Determine access / egress points.
   h. Attempt to obtain blueprints.
   i. Ensure all responding members are wearing body are
   j. Evacuate, secure, and contain the incident site.
   k. Ensure interviews with the evacuated persons are conducted in an attempt to gain information about the suspect(s), injured victims, and trapped people.
   l. Stabilize and coordinate the crime scene with investigative supervisor.
   m. Ensure constant contact and coordination with the Contact Team, Rescue Team, and SWAT.
   n. Not declare the scene under control until a complete search of the building, including roof or substructures has been completed by the SWAT Unit and is declared safe.
   o. Establish a secure cold zone area for witnesses to be housed for investigators.
   p. Ensure the Incident Log was established and maintained.

B. CHANGES IN INCIDENT COMMAND

1. The first deputy on the scene is the Incident Commander until properly relieved by a supervisor.

2. The first Sheriff Office supervisor in route to the scene shall monitor Sheriff's radio to gain information but shall not obstruct ongoing intervention.

3. Command personnel must be on scene and fully briefed before assuming Incident Command.

4. The Philadelphia Police Department SWAT Supervisor will assume tactical Command upon arrival.
5. Sheriff's Radio shall make notification of a change in Incident Command to Police Radio (J-Band) and Sheriff Radio.

V. TRAINING AND EXERCISES

A. Training and exercises are the best activities to help prepare sworn and civilian personnel to react quickly and effectively in emergency situations. When considering training options for establishing awareness and providing appropriate responses to the threat of an active shooter.

1. The Sheriff's Office Uniform Services Deputy Chief shall conduct an annual review of Active Shooter facility plans created by the Facility Captains to identify the best training approach for their facility occupants.

2. This review should assess the specific features of the facility itself along with the needs and capabilities of the personnel occupying the facility.

3. Following the examination of the target population, a needs assessment should be conducted under the assumption that the risk of an active shooter event is high. Therefore, the assessment should formulate the most favorable actions for all persons likely to be involved, including community resources.

B. Exercises: Not unlike periodic fire drills, continual awareness campaigns of the active shooter threat can ensure a much higher chance of reacting quickly and surviving an actual situation.

1. The target population should include individuals occupying or visiting the facility on a day-to-day basis, including security personnel, law enforcement officers, judges, district attorneys, and members of the council and public frequenting the facility.

2. Training participation opportunities should be extended to the external emergency responders likely to support the facility in an active shooter situation.

3. Each target group has different training needs.

   a. For example, members of the general public are less likely to attend formal training and could be exposed to essential information through posters, brochures, or radio and television spot announcements.

   b. Sworn and civilian employees benefit from briefings and participation in active shooter drills.

   c. On-site law enforcement/armed security, as well as external responders, would benefit from hands-on scenario-based training; knowledge of the facilities' physical features such as entrances, exits, and construction features; and knowledge of and familiarity with the capabilities of the internal security force.
4. An active shooter preparedness plan, created annually by each Uniform Services Captain, will be submitted to the Deputy Chief- Uniform Services/Tactical and will become the source document used in the development of a training program in each facility. If no plan exists, the information gained through the need’s analysis will be used to develop a plan. Once needs are identified, a survey of existing training programs should be conducted to determine if a suitable training solution already exists. Often, training needs can be satisfied by an existing program from a sister agency such as FEMA, the PPD, or TSA.

5. Good planning includes conducting exercises with first responders and facility security teams, including any security or law enforcement officers who are employed in the facility. Valuable partners are one of the most effective and efficient ways to ensure that everyone knows not only his or her role but also the role of others at the scene. These exercises should include:

   a. A walkthrough of the facility to allow law enforcement officials to provide input on shelter sites and be familiar with hazardous areas within the facility (e.g., magnetic resonance imaging [MRI] devices and radioactive areas). This will also familiarize first responders with the site, including shelter locations, evacuation routes, and locations where they may find occupants who may be unable to evacuate, such as persons with access or functional needs.

   b. The facility should also consider and plan for how to care for the critically injured from the event. There are many types of exercises, starting with discussion-based exercises such as seminars and tabletop exercises. Activities can graduate to operations-based exercises utilizing personnel and equipment from multiple jurisdictions culminating in a full-scale exercise.

   c. Exercises can be designed to involve the entire facility population, to include local responders, or be narrower in scope to address a smaller portion of the facility or population.

   d. All drills and exercises should be announced prior to conducting them. Some recommendations for exercise programs include:

      1. pre-designated assembly points for people who need assistance evacuating.
      2. verified points of accessible egress.
      3. internal exercise training program for all employees including volunteers to respond to specific assembly areas.
      4. established alert and notification procedures.
      5. pre-determined communications capabilities; and
      6. identify employees who have current and valid credentials in EMS, law enforcement, or fire services that could assist safety or security officers, if needed.

   e. Several active shooter scenarios should be considered because an actual event is unpredictable. Feedback from these exercise sessions is valuable in determining weaknesses in the plan and improving both plans and training.
f. Exercises should be conducted on a recurring basis to keep the active shooter threat fresh in the minds of the participants and should include the latest mitigation techniques and any recent changes in the overall plan.

6. The Deputy Chief, Training shall explore scheduling courses through private sector and non-governmental entities.

C. Instruments

1. In some situations, the uniqueness of the target population may require the design and development of an entirely new training instrument or the modification of an existing one. This could involve the use of professional or experienced instructional designers if sufficient in-house talent is unavailable.

2. The method of instruction delivery depends on several factors.

   a. Instructor-led training is more formal and requires a time commitment from participants for the duration of the course.
   b. In some cases, online or web-based instruction is a suitable alternative that can reduce or alleviate scheduling conflicts or travel requirements.
   c. Posters and other visual aids illustrate key learning points and should be situated in prime locations at the facility. These resources remind facility occupants of the objectives of the training program, strengthen their retention of essential information, and ensure occupants are aware of the possibility of an active shooter event.
   d. The active shooter training video, entitled “Run, Hide, Fight” dramatizes an active shooter incident in the workplace exemplifying the unpredictability and quick evolution of active shooter situations. Its purpose is to educate the public by demonstrating response actions during such an incident so that they can prepare for an active shooter situation.
   e. Active shooter events often appear spontaneous and evolve quickly, therefore preparation is essential. This preparation should include training and planning that maximizes the possibility of survival. In order for information to be actionable, it must be accessible. For example, visual and/or auditory aids and cues (such as posters, sirens, etc.) are only useful if the audience can see and/or hear them. For those with a hearing or visual disability, the information conveyed through these means may not be accessible. Partnering with local disability entities such as Americans with Disabilities Act (ADA) Centers, governor's disability councils, mayoral task forces, independent living centers, etc., for assistance with tools, methods, resources and protocols can make life saving differences for employees and visitors with a variety of access and functional needs or disabilities.

BY ORDER OF:

[Signature]
SHERIFF DATE

42
DIRECTIVE:   #3
SUBJECT:    REASSIGNMENT POLICY
ISSUE DATE: 04-08-2020
REVISED:    02-24-2021

4. PURPOSE:

A. This Directive establishes standardized selection guidelines for the process used to fill all Office of the Sheriff Post vacancies via transfer.

B. The allocation of personnel to a specific assignment is designed to promote efficiency and to optimize departmental effectiveness while considering the needs, knowledge, skills, abilities, and preferences of the individual employees. Although not mutually exclusive, at times both objectives may not be simultaneously achievable.

C. The purpose of this order, the objective of the selection process shall be:

1. Openness, fairness, and objectivity.

2. Impartial assignment opportunities for sworn deputies of all ranks.

D. Definitions

1. **Uniform Operations** - vacancies in uniform services shall be sworn positions responding to and answering calls for service generated by citizens or a supervisor. This designation includes the following positions: deputies/supervisors of all ranks covering all court facilities, transportation duties, bicycle units, and/or posts.

2. **Tactical Support, Training & Administration, Integrity, and Real Estate Sales** - are considered specialized assignments and require sworn personnel who must possess and/or obtain certain knowledge, skills, and abilities in order to accomplish the mission of the division or section.
3. Standardized Selection Process - consists of consideration of all the following criteria for sergeants and below:

1. Letter of intent and resume (preferred),

2. Time and attendance totals (prior twelve (12) months),

3. Performance appraisal (prior twelve (12) months),

4. Internal affairs records (prior twelve (12) months) and,

5. If applicable for uniquely specialized assignments, special fitness, or skill assessments.

6. Board interview


5. Vacancy – for the purposes of this Directive, is an opening within the same rank that would require a lateral reassignment.

5. POLICY:

F. Uniform Operations Vacancies

A. Posting Vacancies: The division experiencing the vacancy shall use at least two (2) methods of communication beyond the department-wide email medium and roll call announcements, which are mandatory. They can utilize an open house, bulletin board postings, etc.) to notify potential candidates as the vacancy moves through each level. Only the Sheriff (or the Chief Deputy) is authorized to fill captain and below Uniform Operations vacancies directly. If vacancies exist within Uniform Operations, then the vacancy shall be offered department-wide, with the selection being made from the first group from which a deputy applies, in the following order:

a. The shift levels.

b. The divisional command (Uniform Operations, i.e., 1501 to CJC., Traffic Court to Widener, City Hall to Warrant Unit, etc., then

c. Department-wide: Requires the vacancy to be forwarded to the Administrative Aide of the Chief Deputy for department-wide posting.

B. Criteria for Application and Selection

a. Each unit, command, and the Office of the Sheriff- Chief of Staff will maintain a seniority list to fill all Uniform Operations vacancies.
b. **Seniority** is the determining factor for shift and assignment, unless the divisional commander articulates documented disciplinary or work performance concerns in most senior interested individual(s) in the twenty-four (24) months preceding the vacancy in writing to their respective Deputy Chief, who must then forward that justification for approval from the Chief Deputy or Sheriff.

6. Requirements and Conditions in Position/Assignment

a. Upon completion of the probationary period, all sworn and certified deputies must serve at least six (6) months in an assigned Uniform Operations Division before being eligible to reassignment to another departmental vacancy. Upon approval of the Uniform Division Captain, the deputy may transfer to another shift/team within their assigned unit during the six (6) month period.

b. All Uniform Operation personnel at the ranks of sergeant and below who desire an assignment out of their division, onto another shift, or any department personnel, who desire an assignment in the Uniform Operations Division, shall submit a request for reassignment to the Uniform Operations Deputy Chief. Any Uniform Operations position at the ranks of lieutenant and below left unfilled shall be posted department wide. The Uniform Operations Deputy Chief shall submit the vacancy to the Chief Deputy Aid who will disseminate the vacancy notification department wide.

c. All newly promoted or newly transferred sergeants must serve a minimum of one (1) year in the following capacities, Uniform Operations, Desk Sergeant, Transportation Sergeant, and/or a Detention Unit Sergeant assignment.

d. In the case of a reduction in force or a demotion, either voluntary, or because of disciplinary action, the Chief Deputy may direct the opening of unfilled/frozen positions in Uniform Operations. This allows for the demoted, and those displaced, to use seniority as a basis for placement into a new position, as if they were members of the Uniform Operations workgroup experiencing the vacancy.

7. **PROCEDURE:**

A. Specialized Services Vacancies

1. Posting Vacancies

   a. All postings for a specialized assignment will require at least a one (1) year commitment before being eligible for a voluntary transfer.

   b. Any vacancies for the ranks of sergeant and below created by personnel reassignment will require a department-wide vacancy announcement following the Standardized Selection Process in II-A.

   c. The division Deputy Chief or designee experiencing or anticipating a vacancy for the rank of sergeant and below shall notify the Administrative Aid of the Chief Deputy in writing, of the vacancy; the criteria for applicant consideration, and any
special or specific criteria or information that is likely to influence potential applicants.

d. The division Deputy Chief or designee shall host at least one open house/interest meeting for potential candidates to meet with the supervisors/staff of the unit experiencing the vacancy to learn the scope of work and responsibilities of the position. The date, time, and location of the open house/interest meeting shall be included in the vacancy announcement and conducive to persons interested working all shifts.

e. If only one potential applicant responds, and the applicant is suited for the position, then no formal standardized selection process interview or reposting of the vacancy is necessary. A memorandum will be required from the posting division to the Chief Deputy naming those persons who hosted and attended the open house and any others expressing interest in the position before the vacancy is filled.

f. In all cases where more than one potential applicant responds in writing indicating an interest in the position, then a formal selection process, including an interview shall be initiated.

g. The Administrative Aid for the Chief Deputy shall distribute the vacancy announcement within three (3) days upon receipt of the necessary information via email (posting). Vacancy announcements must be posted, and letters of interest accepted for at least fourteen (14) calendar days prior to the closing date.

h. All vacancy announcements shall comply with EEO regulations. The Sheriff’s Office Human Resources Director is available for consultation and review of standardized interview questions, if requested, to ensure EEO compliance.

2. Criteria for Application and Selection

a. Personnel interested in consideration for the announced vacancy position are responsible for submitting all information requested in the vacancy announcement as directed to the unit/division experiencing the vacancy within the application period.

b. After the closing date of the posting, the commander or supervisor of the unit or section experiencing the vacancy shall review the submitted materials to determine which, if any, of applicants are qualified for the position. Interviews shall be conducted and shall include all applicants who meet minimum requirements for the open position. The interviews will be completed within seven (7) working days after the closure of the vacancy posting unless an exigent situation occurs. If an exigency exists, the posting commander will prepare a memorandum explaining the cause of the rescheduling and include descriptions of when and how interviews will be completed in a timely manner.

1. The unit supervisor shall ensure Human Resources Director staff reviews and approves all standardized interview questions prior to conducting the interviews.
2. The HR Director shall determine which interview questions will be used, in what order, and only reveal the questions to the interview board on the date of the interviews.

3. The interview panel shall consist of members of the unit experiencing the vacancy, the unit’s chain of command, and/or individuals with expertise in skills and abilities required in the unit for a maximum of three (3) internal panelists. The Deputy Director of HR will personally observe each interview panel for uniformity, consistency, and strict adherence to this directive.

4. The interview panel should have the overarching goal of inclusivity. The board shall be comprised of diverse department personnel that closely reflect the demographics of the community; therefore, additional members outside of the unit experiencing the vacancy may be requested to sit on the panel to fulfill this goal. Each panelist selected shall attend all interviews for the vacant position, have scoring responsibilities, and will participate in the evaluation of candidates.

1. Members of the interview panel will use a standardized Interview Assessment Form developed by the HR Department to record their evaluation of each candidate.

c. The applicants shall be placed into an applicant pool. No numeric ranking shall be assigned, nor any numeric score calculated to determine placement onto a recommendation list. Unless stated otherwise in the vacancy announcement, any recommendation list will be valid for 365 days from the date it is created for the purposes of filling subsequent vacancies. After 365 days, the recommendation list will be voided, and a new selection process will be required to fill subsequent vacancies.

1. The unit supervisor will submit a memorandum with recommendations through the chain of command to the Chief Deputy, along with the Standardized Scoring Sheet and all documents used to evaluate the candidates.

2. The memorandum shall list all applicants, and indicate whether each person is either “qualified” or “not qualified.” For those deemed not qualified, an explanation shall be provided on the memo and subsequently forwarded through the chain of command to the applicable Deputy Chief.

3. The chain of command can disregard the commander’s or supervisor’s designation of a candidate as being qualified or not qualified.
4. The chain of command shall consider the needs of the community, specific organizational problems, and other specific needs of the unit/division experiencing the vacancy when choosing an applicant for the position.

5. Guidelines for the Office of the Sheriff’s goal of creating and maintaining a diverse workforce that is in the best interest of the department, employees and the community should be a factor in every selection process.

c. For a position vacancy in a specialized assignment, the final approving party shall be the Chief Deputy, after receiving a written recommendation from the Deputy Chief in command of the area experiencing the vacancy. Upon completing the review, the Chief Deputy shall submit all documents related to the selection process to the HR Director for retention of those documents in accordance with the City’s retention schedule.

d. Unless the Deputy Chief over the bureau experiencing the vacancy articulates documented disciplinary or work performance issues with the recommended individual(s) occurring within the twenty-four (24) months preceding the vacancy the report will be forwarded to the HR Department Director for review of compliance with EEO guidelines. Upon notification of compliance from the HR Department Director (or designee), the original approving party will designate captain to contact the candidate selected for the position.

1. The captain or designee shall provide feedback to unselected candidates to enhance the candidate’s future viability for selection within ten (10) days of the conclusion of the selection process.

B. Administrative Aides or Executive Assistants

1. Appointed ranks (Deputy Chiefs and above) may choose an administrative deputy/aide based on their determination of what is best for their command and the Office of the Sheriff.

2. Executive Assistants are civilian exempt positions that require budget approval, therefore require the approval of the sheriff.

3. Vacancies in other administrative positions will be filled in accordance with the Standard Selection Process.

C. Supervisory Assignments

1. Shift supervisory assignments in Uniform Operations shall be filled by seniority unless the Deputy Chief or Chief Inspector articulates documented disciplinary or work performance issues with the most senior supervisor within that rank that have occurred
in the preceding twelve (12) months. The Chief Deputy shall approve any variations from seniority-based assignment placement.

a. Special consideration shall be given to those who have volunteered to work rotating and evening/night shifts over the prior year.

2. All newly promoted supervisors shall be assigned to Uniform Operations. There is no time restriction on when a newly promoted supervisor may express interest in, or be considered for, other positions.

3. The Executive Staff (Sheriff, Chief Deputy, Undersheriff, and Chief of Staff) will determine specialized services supervisory assignments.

a. The Transportation Supervisors, Desk Sergeant, K9 Supervisor, and Bike Supervisor in the Uniform Operations Division are considered specialized services positions.

b. Supervisor positions in the Tactical Support Bureau, Training and Administration, and the Integrity & Real Estate Sales Bureau(s) are considered specialized services positions.

4. Supervisors in specialized services shall serve no more than four (4) years in an assignment.

a. The Chief of Staff and Human Resources Director are responsible for monitoring the tenure of supervisors in specialized services positions.

b. The Chief of Staff and Human Resources Director staff will notify the Executive Staff when a supervisor has served three (3) years in a specialized assignment so the process of transitioning/cross-training that position to a different supervisor can be initiated without tumult.

D. Selection of the assignments for the rank of captain is at the sole discretion of the executive staff. The Standardized Selection Process will not be utilized for this rank.

E. In cases where an emergency exists or promotions/demotions require that immediate assignments be made, sworn personnel may be placed in temporary positions until such time as the selection process may be conducted in order to permanently fill the position(s).

F. In cases where there are no applicants for a position or where the available applicants are not qualified for the position, other means may be used for the selection of personnel to fill the vacancy, upon approval by the Sheriff.

G. As per this directive, approved transfers must be received by the Human Resources Director no later than 1700 hours, Friday, two (2) weeks preceding the effective date of the transfer. In an effort to assure that vacancies remain evenly distributed throughout the
Office of the Sheriff, the effective date of transfers shall be restricted to once per quarter for all ranks below the rank of Lieutenant. Transfer dates shall be designated by Command Staff but will generally fall in the mid-month of any fiscal quarter. An exception is permitted upon agreement between the deputy chiefs or above over the releasing and receiving units.

H. Performance-based rotation guidelines shall be developed for officers assigned to the Warrant Unit and Task Forces. At the end of three years in the assignment, officers of the rank of lieutenant and below shall be subject to a yearly performance-based rotation review to determine their suitability for continued assignment in the section.

I. The Sheriff enjoys the discretion to deviate from the requirements of this Directive when the Sheriff determines that it is in the best interest of the Department. Transfers and assignments made by the Sheriff are not subject to grievance under the FOP contract.
DIRECTIVE: #4
SUBJECT: UNIFORM AND EQUIPMENT POLICY
ISSUE DATE: 04-08-2020
REVISED DATE: 02-24-2021

8. PURPOSE:

A. This directive establishes Uniform Standards for employees of the Office of the Sheriff. All sworn personnel will maintain a clean, neat, and well-groomed appearance in their dress and deportment. All equipment will always be maintained in good working condition and kept clean, presentable, and secure. Daily inspections will be conducted by supervisory personnel.

B. All personnel will maintain the prescribed uniform regardless of their assignment. Clothing covering the face in a manner that would prevent an officer from being identified unless such concealment is consistent with a current assignment is strictly prohibited. Personnel assigned to specialized units must have the basic prescribed uniform and equipment readily available.

C. Sworn deputies will report for roll call at the specified time prescribed in complete uniform of the day and fully prepared for duty. Personnel not complying will be granted leave without pay or holiday/vacation time in order to come into compliance.

D. Deputy Chiefs will conduct a uniform clothing inspection in August of each year.

E. No member of the Office of the Sheriff is permitted to sell, give, exchange or trade, a firearm, ammunition, weapon, uniform and/or uniform equipment, or any part of the uniform and/or equipment to any person who is not an Office of the Sheriff Deputy without written authority of the Sheriff of Philadelphia.

F. No member of the Office of the Sheriff will accept/solicit restitution for uniform(s)/equipment damaged in the performance of duty, or through negligent acts by the deputy to which the uniform or equipment is issued.
G. All sworn members of the Office of the Sheriff shall carry the firearm issued/approved for carry by the Firearms Training Unit Technician, while on duty. This will be the firearm with which s/he has qualified on an annual basis and is the ONLY firearm that shall be carried on duty. Ammunition used for firearms must be issued or approved by the Training Unit.

1. The carrying of non-issued weapons on duty is prohibited.

2. When employees’ issued firearms retire or separate, the employee will surrender all individually issued firearms to the Firearms Technician who log the item back into the Armory Inventor Telesoft Record and will ensure the Training Captain updates the training records.

H. All personnel assigned to a limited duty status will wear appropriate civilian attire, according to their assignment, including trousers, shirts, and ties for men; dresses, suits or slacks for women. Jeans and tee shirts are not appropriate attire.
NOTE: This also applies to personnel in sick/injured status and plainclothes / investigatory personnel who are required to appear in court.

9. PRESCRIBED UNIFORM:

A. Sworn personnel in the Office of the Sheriff shall wear and carry such equipment such uniform and insignia as the Sheriff may prescribe.

1. In addition to the standard deputy uniform described below, uniform shall be defined to include any clothing, footwear, headgear, etc., worn on-duty while carrying out assigned duties and shall include, but not be limited to, raid outfits, shirts with a facsimile of the Sheriff’s badge and the word “Sheriff” on it or the name of a functional entity of the department, helmets and six-pocket pants.

   a. Only insignia, patches, monograms, emblems, or other markings stated as approved in this directive shall be permitted on any visible uniform item. Commercial emblems, markings, brands, slogans, logos, or other insignia are prohibited on any visible uniform item.

   b. No alternate uniform, or alternate uniform item, shall be worn unless specifically provided for in Specialized Units Uniform Requirements.

2. Alternate uniforms may have items such as nameplate, badge, pins, and patches which are embroidered on the uniform for tactical purposes and, if so specified in Specialized Units Uniform Requirements that may be excluded from the requirements to wear the standard uniform item.

3. Guidelines prescribed in this directive pertaining to the care, appearance, and wearing of the uniform or any accessory or hair style shall also apply to alternate uniforms and headgear.
4. Any officer with a medical necessity to vary from the standard or alternate uniform, including uniform items, shall have the medical documentation on file with the Human Resources Director and Chief Deputy.

5. All equipment issued to a deputy is the property of the Office of the Sheriff and is subject to inspection at any time. When sworn personnel leave the Office, all Office property shall be returned immediately.

6. All uniformed personnel shall report for roll call in the complete standard deputy sheriff uniform as prescribed in this order. No employee assigned to wear the uniform shall report to duty in civilian clothing without their supervisor’s permission.

7. Uniforms shall be kept neat, clean, well pressed, and in good condition at all times. Leather goods shall be kept in good condition to include maintenance with polish on a regular basis. A complete standard police uniform inspection, including uniform cap, shall be conducted in accordance with each unit or section's standard operating procedures.

8. There is an established period for wearing either the summer or winter standard deputy uniform. Both long-sleeved and short-sleeved shirts are approved by the Sheriff throughout the year, however, the wearing of the summer and winter Garrison hats are interchangeable.

9. The uniform shall not be worn off duty except when:
   a. Traveling to and from work.
   b. Appearing in court when subpoenaed in a work-related capacity.
   c. Engaging in an off-duty Law Enforcement capacity as approved by the Sheriff.

B. Only the uniform cap, or bicycle helmet/cap approved shall be worn, unless an exemption is provided for in directives, Specialized Units Uniform Requirements, or by Special Order.

1. The bicycle helmet/cap may only be worn by deputies assigned to bike patrol or K-9.

2. The uniform cap shall be worn:
   a. Level on the head as viewed from the front and back, and with the front tip of the cap bill level with the top of the eyebrows as viewed from the side.
   b. Uniformed sergeants shall have a silver-colored scroll mesh cap strap and frontispiece.
   c. Lieutenants and above shall have a gold-colored scroll mesh cap strap and gold cap frontispiece.
   d. Appropriate gold or silver cap frontispieces shall be centered in front of the cap and ¼ inch below the top seam.
3. Deputies may wear only the approved headgear when working all indoor assignments except places of worship.

4. All rules regarding wearing of the Sheriff Office uniform, including headgear, are applicable whether the deputy is wearing the uniform on or off duty.

5. When duties permit, while in uniform and wearing the uniform cap or bicycle helmet, deputies shall salute the national colors during public occasions, ceremonies, or parades. During the playing of the national anthem, deputies shall stand at attention, face the flag, and maintain a military salute. When no flag is presented, members shall face the direction of the music while saluting. When deputies are not wearing the approved cap or headgear, or while in civilian attire, they shall not salute but shall stand at attention and place their right hand over their heart.

   a. Officers, who are members of the Armed Forces or veterans who are present, but not in uniform, may render the military salute as provided by the United States Code.

6. When duties permit, the uniform cap or bicycle helmet/cap should be removed at events where invocations or prayers are offered, in court rooms and always where proper decorum should be maintained. Deputies shall show proper respect at funerals by placing their headgear over the left chest when passing the casket. Uniformed deputies on escort duty shall come to attention and salute the hearse and family cars when, duties permitting.

C. Uniform personnel and personnel required to have uniforms will present for annual inspection, in good condition, the following items:

1. Leather Coat or Patrol Jacket

   a. In lieu of the Patrol Jacket, the reversible VizGuard™ S315VP - Duty Jacket, dark side out, may be worn. The metal deputy sheriff badge of rank, departmental and unit patches, and rank insignias (including city seals for the rank of Lieutenant and above) will be worn. Names will be stitched, embroidered, or name tags sewn onto garment (no smaller than 1/2 inch, no larger than 3/4 inch white lettering) may be used. All name designations will be centered directly above the metal deputy sheriff badge of rank.

2. Blouse Coat (Lieutenants and above; optional for Sergeants and below)

3. Four (4) pairs of Trousers

4. Two (2) Long Sleeve Blue Shirts (White for Sergeant and above)

5. Two (2) Short Sleeve Blue Shirts (White for Sergeant and above)

6. Winter Hat/Summer Hat

7. Raincoat: long style: yellow (black for Lieutenant and above)
8. Garrison Belt (Black Leather); nylon may be used but not with formal uniform.

9. Handcuff Case or Handcuff Clip (Black Leather); nylon may be used but not with formal uniform.

10. A pair of shoes, black-laced plain toe, military type, or Police Tactical Boot

11. Black Tie (2 3/4 inches wide)

12. A Pair of Black Leather Dress Gloves (No cut-offs, driving gloves, football, or baseball batting gloves, etc.)

13. Three (3) Nameplates

14. Protective Vest: Ballistic vests will be worn by all sworn personnel, and if exposed, must be white and clean.

D. Members are forbidden to exchange parts of uniforms for the purpose of passing inspection.

E. The inspecting supervisor/commander will instruct the employee to replace any items not meeting departmental standards. Articles must be clean, neat fitting and not frayed or worn.

F. Each description below designates the regulation uniform, any one of which maybe specified as the official uniform of the day based on the prevailing weather.

1. Regulation Uniform #1

   a. Summer/Winter trousers; short sleeve blue poplin shirt; Summer/Winter hat.
   b. The following short sleeve knit uniform shirt has been approved as an option for the ranks of Lieutenant and below.

      1) Optional Models:

         i. Style K5103-Elbeco UFX SS Knit Uniform Shirt (Blue)
         ii. Style K5100-Elbeco UFX SS Knit Uniform Shirt (White)
         iii. Style #0368/Blue-Class “A” Polo Shirt (Blue)
         iv. Style #0368/White-Class “A” Polo Shirt (White)
         v. Style #342/Phila- Olympic Polo Class “A” Shirt

2. Regulation Uniform #2

   a. Summer/Winter trousers; long sleeve blue poplin shirt; black tie; Summer/Winter Hat.
b. The following long sleeve knit uniform shirts are an option for the ranks of Lieutenant and below, Uniformed Services personnel only. The long sleeve versions of this shirt will be worn with the layer mock turtleneck dickie underneath. Under no circumstances will the long sleeve knit shirt be worn without the dickie as an open-collared shirt.

1. Optional Models:

   i. Style K5163-Elbeco UFX LS Knit Uniform Shirt (Blue)
   ii. Style K5160-Elbeco UFX LS Knit Uniform Shirt (White)
   iii. Style #0369/Blue-Class “A” Polo Shirt (Blue)
   iv. Style #0369/White-Class “A” Polo Shirt (White)
   v. Style #342/Phila- Olympic Polo Class “A” Shirt

c. Mock Turtleneck Models: Style #8930-UFX Performance base layer mock turtleneck dickie (Black/White). “PSO” to be embroidered left of center neck. Style #6140-East Valley apparel layer mock turtleneck dickie (Blk/Wh). “PSO” to be embroidered left of center neck.

3. Regulation Uniform #3

   a. Summer/Winter trousers; long sleeve blue poplin shirt; black tie; blouse coat/patrol jacket; a tactical sweater under jacket or as outermost garment; Winter/Summer hat; Sam Browne belt and holster (with blouse coat); Sergeants and below.
   b. The smaller rank insignia for the rank of Lieutenant and above will be centered above the collar point of the uniform shirt. This will be in lieu of the insignia worn on the shoulder of the uniform shirt.
   c. The following long sleeve knit uniform shirts are an option for the ranks of Lieutenant and below, Uniformed Services personnel only. The long sleeve versions of this shirt will be worn with the layer mock turtleneck dickie underneath. Under no circumstances will the long sleeve shirt be worn without the dickie as an open-collared shirt.

1) Optional Models:

   i. Style K5163-Elbeco UFX LS Knit Uniform Shirt (Blue)
   ii. Style K5160-Elbeco UFX LS Knit Uniform Shirt (White)
   iii. Style #0369/Blue-Class “A” Polo Shirt (Blue)
   iv. Style #0369/White-Class “A” Polo Shirt (White)
   v. Style #342/Phila- Olympic Polo Class “A” Shirt

d. Mock Turtleneck Models:

   i. Style #8930-UFX Performance base layer mock turtleneck dickie (Blk/White). “PSO” to be embroidered left of center neck.
ii. Style #6140-East Valley apparel layer mock turtleneck dickie (Blk/White). “PSO” to be embroidered left of center neck.

e. The following unisex Patrol Jacket & Liner is an option for all ranks:

i. Public Safety Gore Tex Jacket & Liner (Unisex) Flying Cross by Fechheimer, Item #79901

ii. GTX-Police Newport Harbor by Whaling Distributors Inc. Jacket & Liner (Unisex), Item #02289

f. Optional Leather Jacket Models:

i. Taylor's Leatherwear (Unisex) Style “Pursuit II” Item #G1010Z

ii. Taylor's Leatherwear (Unisex) Style “Indianapolis” Item #4461Z

4. Regulation Uniform #4

a. Summer/Winter trousers; mock turtleneck shirt or long sleeve blue poplin shirt with black tie; patrol jacket/leather coat; winter/summer hat - trooper type fur cap (black) may be worn 32 degrees or below; gloves may be worn. Tactical sweater may be worn under patrol jacket/leather coat.

b. The smaller rank insignia for the rank of Lieutenant and above will be centered above the collar point of the uniform shirt. This will be in lieu of the insignia worn on the shoulder of the uniform shirt.

c. The quick draw type holster may only be worn with Uniforms #1 and #2 and may not be worn with the patrol jacket. When the patrol jacket is worn, the Sam Browne belt will not be worn.

d. The following long sleeve knit uniform shirts are an option for the ranks of Lieutenant and below. The long sleeve versions of this shirt will be worn with the layer mock turtleneck dickie underneath. Under no circumstances will the long sleeve shirt be worn without the mock turtleneck as an open-collared shirt.

1. Optional Models:

i. Style K5163-Elbeco UFX LS Knit Uniform Shirt (Blue)

ii. Style K5160-Elbeco UFX LS Knit Uniform Shirt (White)

iii. Style #0369/Blu-Class “A” Polo Shirt (Blue)

iv. Style #0369/White-Class “A” Polo Shirt (White)

v. Style #342/Phila- Olympic Polo Class “A” Shirt


i. Style #6140-East Valley apparel layer mock turtleneck dickie (Blk/White). “PSO” to be embroidered left of center neck.
e. The following unisex Patrol Jacket & Liner is an option for all ranks.

1. Optional Jacket Models:
   i. Public Safety Gore Tex Jacket & Liner (Unisex) Flying Cross by Fechheimer, Item #79901GTX-Police.
   ii. Newport Harbor by Whaling Distributors Inc. Jacket & Liner (Unisex), Item #02289

2. Optional Leather Jacket Models: Taylor’s Leatherwear (Unisex)
   i. Style “Pursuit II” Item #G1010Z
   ii. Taylor’s Leatherwear (Unisex) Style “Indianapolis” Item #4461Z

5. Regulation Uniform #5 (Cell Room-Deputies):
   a. Cell room deputies may wear approved navy/blue Tee shirt, Golf, alternate uniform, sweatshirt, or fleece jacket with Sheriff's Office badge embroidered over the left breast and navy/blue BDU pants (Standard duty uniform must be available for other assignments.)

6. All deputies assigned to Special Units (K-9, Bike Patrol, SOG, Detention Unit must be in their respective Units prescribed uniform. The uniform must be in working order and readily accessible in event that emergency deployment becomes necessary.

7. Service weapon - worn on dominant side, butt of the weapon to the rear.

8. Non-Uniformed/Plainclothes: Appearance
   a. Personnel, both sworn and non-sworn, assigned to non-uniformed positions shall wear clothing which presents a professional businesslike appearance. Business casual shall be appropriate throughout the year on normal business days that do not require activities such as court appearance, council meetings, meetings with businesses, or any official department function or ceremony that would require more formal business attire or the full-dress uniform.
   b. Business Casual

1. Male employees are not required to wear a tie and have the option of a long or short-sleeved collared shirt.

2. Traditional dress shirts, banded-collar dress shirts, and knit shirts with jacket and collar (i.e. polo shirts) are approved for business casual wear.
   i. Polo-styled shirts may have the official City of Philadelphia/Office of the Sheriff emblem with "Sheriff" (sworn personnel) or "Sheriff's Department" (non-sworn personnel) embroidered on the left side of the
shirt. Polo Shirts with a printed or embroidered badge or patch are not permitted for non-sworn personnel.

3. Deputies shall ensure their badge or clothing displaying the approved Sheriff’s Office logo is clearly visible when a jacket is not worn, and their firearm is not concealed.

c. Business Attire: Male administrative employees shall wear both a suit or sport coat and slacks with a dress shirt and tie. Female employees shall wear a dress, business suit, pants suit, or a skirt (or slacks) with blouse, sweater, or jacket. Male and female sworn administrative staff may wear business attire when authorized by the Sheriff or designee.

d. Inappropriate clothing, including footwear (i.e., sneakers, tennis shoes, golf shoes, high heels, sandals, slippers, etc.). Clothing with offensive slogans or expletives are forbidden. No employee may wear skin-tight, spandex, or stretch fabric clothing in the workplace or in the course of duties for the Office of the Sheriff. Exceptions to non-uniformed dress standards for officers in specialized assignments may be granted by the appropriate Deputy Chief.

e. Deputies actively engaged in an undercover assignment are exempt from these rules and will dress in a manner determined by their supervisor.

f. Non-sworn personnel assigned to divisions having a specific uniform will follow the division’s guidelines for wearing of the uniform.

G. Other clothing and accessories, when worn with the official prescribed uniform, will conform to the following:

1. Socks - black or dark blue

2. Neckties - black, four-in-hand or “redi-knot” (not knitted).

3. Undershirts - optional, must be white, if exposed when worn with short sleeve, open collar uniform shirts.

4. Shoes

   a. Black laced plain toe dress type or Rocky Police Tactical Boot. Shoes worn with uniform must be black, smooth-grained leather or similar synthetic material having an acceptable likeness to leather. The shoes may be low cut or high top and must have black stitching and black edged soles. Heels, measured from the top of the sole to the bottom of the heel, shall not exceed 1 ½” in height. Only shoes with eyelets and shoelaces shall be worn.

   b. Shoes bearing stripes, commercial emblems or other insignia are prohibited.
c. Loafers, wing tips, or shoes with buckles or straps are not acceptable for wear with the deputy sheriff uniform.
d. Shoes shall be polished at all times. Shoes shall be in a good state of repair, at all times.

5. Black overshoes may be worn in inclement weather.

6. Scarves - black or navy blue only. Captains and above may wear white scarves.

7. Sweaters - Jack Young Commando V-Neck, Style 4000 (black). All other sweaters are black or navy blue only. No turtlenecks or crew necks permitted. The appropriate dress shirt and tie will be worn when wearing a sweater.

8. Jewelry - restricted to wedding band, watch, tie clasp, identification bracelet, class ring and medical alert bracelet or medallion.
   a. No "visible" necklace/medal or body piercing jewelry (including on the tongue) may be worn while on duty. All sworn male personnel will not be permitted to wear earrings while on duty.
      i. Exception: Female officers with pierced ears may wear one pair of small post type earrings, no more than 1/4" in diameter. They shall not dangle below the earlobe, protrude or be worn above the earlobe. No more than one (1) earring per ear may be worn.
      ii. Earlobe gauges are considered body piercing jewelry and are not permitted to be worn while on duty by sworn members of the department.

9. Rubber (water resistant) issued Boots

10. Ballistic Vest Outer/ Inner- Carrier worn over prescribed uniform:
   a. Blue or Black Vest Outer Carrier: PSO
   b. White Vest Outer Carrier: Supervisors

11. Earmuffs - black/navy worn when temperature is below freezing (32 degrees).

12. Eyewear-Mirror lenses and brightly colored frames and wraparounds are not permitted.

13. Mock turtleneck shirt, (Black – Corporals and below) (White – Sergeants and above). PSO embroidered in 1/2" block letters on collar (White – Corporals and below) (Black – Sergeants and above)
   a. Embroidered "PSO" is the only designation permitted on the collar.
14. Service markers may be worn 4-1/2" from the end of left sleeve: For every (5) years of service, one (1) hash mark (medium gold bar with black background) may be worn. Example: 20 years of completed service - (4) hash marks.

15. The Office of the Sheriff Star will be worn on the left sleeve on patrol jackets, leather coats, blouse coats, tactical sweaters and uniform shirts approximately 1" down from the shoulder seam.

   a. Unit or district approved shoulder patch insignia will be worn on the right sleeve approximately 1" down from the shoulder seam.
   b. Sergeants and Corporals will attach the reduced size patch on uniform shirts, approximately 1/2" down from the shoulder seam.
   c. All other garments will have the regular patch attached 1" down from the shoulder seam.

16. Ranking officers' coats will display:

   a. Two (2) City Seal Pins - to be worn centered on the collars of the coats, approximately 5/8ths of an inch above the cut of the lapel. However, City Seal Pins will not be worn on the fur collar of patrol jackets.

   b. Rank insignia - to be worn on both shoulder loops, approximately 5/8ths of an inch from the outer shoulder seam.

      1) The insignias are:

      i. Sheriff-Four Gold Stars
      ii. Chief Deputy-Three Gold Stars
      iii. Deputy Chief-Two Gold Stars
      iv. Chief Inspector-Gold Spread Eagle
      v. Inspector-Silver Metal Oak Leaf
      vi. Staff Inspector-Gold Metal Oak Leaf
      vii. Captain-Double Gold Bars
      viii. Lieutenant-Single Gold Bar
      ix. Sergeant and Corporal Stripes - to be worn on sleeves, directly below patch(es) on shirts, blouse coats, patrol jackets, tactical sweaters, and leather coats. Stripes will be worn parallel to each other.

H. Personnel replacing original uniform clothing or purchasing additional items will ensure that such replacement clothing conforms to the styles and colors of the original uniform clothing items issued by the Office of the Sheriff Training Division to new recruits. These uniform items are the standard for the Office of the Sheriff and replacement items must be the same or an equivalent. Any deviations will be unacceptable.
I. Commanding Officers of units requiring specialized clothing items (Warrants, etc.) will ensure that newly assigned personnel are made aware of the required styles and colors of the specific clothing items.

10. **WEARING THE UNIFORM**

A. The uniform identifies a police officer as a professional law enforcement agent and is to be in good condition, clean, well pressed, and always buttoned.

B. The following regulations will be followed:

1. Shirt collars and cuffs will be clean, buttoned, and the tie properly adjusted/aligned in the center of the body. Outer garments will always be buttoned or zippered.

2. Leather goods and shoes will be cleaned and polished.

3. Ammunition carrier - To be worn in the front, either side of the buckle.

4. Hats will be worn in a military manner with frontispiece attached when out of a vehicle. Ultimately, the hairstyle is secondary to the proper wearing of the hat.

5. The Sheriff Badge and frontispiece will be cleaned and polished.

   a. The Sheriff Deputy badge will be worn on the outermost garment over the left breast.

6. Nameplates will be on the outermost garment (except raincoats) on the right side of the breast directly above the pocket. On garment not having breast pockets, they are to be on the right side on a horizontal plane with the badge.

   a. Nameplates are to be worn directly above the badge on leather coats and patrol jackets.

7. An American Flag pin is an optional and authorized piece of equipment. When worn, it will be placed next to the name tag on the side closest to the center of the chest.

8. All sworn Deputies are permitted to wear non-City issued service pins and awards above the name tag on the right side of the uniform.

9. S.O. Commendation Ribbons:

   a. Ribbons will be worn in the color designations indicated, centered above the badge as follows:

      1) Valor – Purple
      2) Bravery – Red
      3) Heroism – Green
4) Excellence -- Red and Blue
5) Merit -- Blue
6) Commendatory Citation -- Gold/Blue/Gold

b. When worn with the leather coat or patrol jacket, the ribbons will be placed above the nameplate.

c. When ribbons for all six (6) categories are worn, they will be worn two (2) abreast for a total of three (3) rows. The highest (Valor) will be worn on the top row, closest to the heart with the 4th highest (Excellence) to the left. On the second row, Bravery will be worn closest to the heart, Merit to the left. On the bottom row, Heroism will be worn closest to the heart, Commendatory Citation to the left.

d. When ribbons for five (5) categories are worn, the highest will be worn at the top, centered above the other four ribbons, which will be worn two abreast for a total of three (3) rows. On the second row, the second highest ribbon will be worn closest to the heart with the 4th highest to its left. On the bottom row, the third highest ribbon will be worn closest to the heart, with the lowest ribbon to its left.

e. When four (4) ribbons are worn, they will be worn two (2) abreast for a total of two (2) rows. The highest will be worn on the top row, closest to the heart with the third highest to its left. On the bottom row, the second highest ribbon will be worn beneath the highest with the lowest ribbon to its left.

f. When three (3) ribbons are worn, the highest ribbon will be worn centered above the other two. The next highest will be worn on the bottom row, closest to the heart, with the lowest ribbon to its left. With two (2) ribbons, the highest will be worn closest to the heart.

g. Subsequent commendations, including Commendatory Citation, for the same category will be designated by stars and oak-leaf clusters.

1) 3/16" star = 1 additional commendation
2) 5/16" star = 5 additional commendations
3) oak leaf cluster = 20 additional commendations
4) Stars and oak leaf clusters will be displayed on the ribbons in an orderly fashion.

10. RNC PIN-If applicable-The red, white, and blue 2000 Republican National Convention Ribbon, Super Bowl, Papal or other special recognition pin(s) will be worn centered below all other commendation ribbons. When no commendation ribbons are worn, it will be worn centered above the badge. If worn with the leather coat or patrol jacket, it will be worn above the nameplate.

11. The green, yellow and blue Military Veteran’s Ribbon will be worn in a higher order than the 2000 Republican National Convention Ribbon but below all other commendation ribbons. When no commendation ribbons or the 2000 Republican National Convention ribbon are worn, it will be worn centered above the badge.

12. Wearing of Commendation Medals
a. Commendation medals may be worn on the blouse coat during formal occasions, such as ceremonies and funerals.

b. Medals will be worn on the left-hand side of the blouse coat under the badge on the seam of the pocket.

c. Medals will be worn in the order listed for the corresponding ribbons.

d. The Medal of Honor which is awarded to the family of a fallen officer will not be worn on the uniform.

13. District/unit pins will be worn on shirt collars only, approximately 5/8" from point of collar.

a. EXCEPTION: The rank of Lieutenant and above will not wear the unit pin on the collar point of the uniform shirt while in uniform #3 and #4, as this is where the rank insignia will be worn.

14. Unless listed in this directive, no other device, badge, button, insignia, or item, except those specifically authorized by the Office of the Sheriff, will be worn, or displayed on the official uniform.

15. The black mourning crepe will be worn on the badge only with authorization of the Sheriff’s Office and for a period of only 30 days. Black tape will not be used as a mourning crepe.

C. Plainclothes personnel will be clean and neat and attired in an appropriate fashion consistent with their assignment (see II-F).

11. **HAIRSTYLES**

A. Male Deputies:

1. Haircuts - hair must be neat, combed, clean, and may be corn-rowed, dreadlocked, and cut into styles that do not distract from personal appearance or touches the collar or stick out around the hat. Hair may touch the top of the ears but may not cover any portion of the outside of the ear. It must be worn in such a manner that it does not interfere in any way with the proper wearing of the uniform hat in the accepted military manner.

2. Sideburns - will not extend lower than the top of the earlobe.

3. Mustaches - when worn, will be neat and trimmed at all times, ending in a straight line from the corners of the mouth.

4. **Beards and goatees - are not permitted** except when consistent with assignment, and the following exceptions:
a. **Medical Exception** - A beard may only be worn for health reasons when a waiver is authorized by the Sheriff based upon the advice of the City’s Medical Director that the employee has a medical condition that prevents him from shaving. If a waiver is authorized, facial hair will be kept trimmed and neat, not to exceed \( \frac{1}{4} \)" in length. Individuals granted a waiver shall be monitored and reviewed by the Medical Director every three (3) months to determine if the medical condition persists to warrant the continuation of the waiver.

b. **Religious Exception** - A beard may be worn when a waiver is authorized by the Sheriff. A waiver will only be authorized upon submitting documentation from the employee by his religious representative that the employee practices a religion that requires him to wear a beard. The request for a waiver must have the name of the religion, the specific beard requirement and must be on the religious institution’s letterhead. The documentation must be notarized or subject to verification. If a waiver is authorized, facial hair will be kept trimmed and neat, not to exceed \( \frac{1}{4} \)" in length. Waivers will expire after 12 months and employees must reapply at the end of each term.

B. Female Deputies:

1. Hair - hair may be worn in professional contemporary styles but will not extend below the bottom of the collar and will conform to the following:
   
   a. Hair must be neat, combed, clean, and may be corn-rowed, dreadlocked, and cut into styles that do not distract from personal appearance.
   
   b. Hair may be worn over the ear but will not extend below the earlobe. No hair will show or extend over the forehead below the cap. Hair may be pinned up in order to meet these requirements.
   
   c. No hairstyle may interfere with the proper wearing of the uniform hat in the accepted military manner.

   1) The grooming and style must be maintained under all but the most adverse conditions. Longer hair must be fashioned in a way that it does not extend outward from the scalp more than \( 1\frac{1}{2} \)" in length and never below the bottom edge of the shirt collar. Braiding, twisting, and locking hairstyles are permitted provided they are well kempt and have a professional appearance.

2. Cosmetics - While on duty, cosmetics, including lipstick may be applied lightly. The colors may neither be too bright nor too dark. False eyelashes may not be used.

3. Fingernails - Cannot be longer than one-eighth (1/8) of an inch from the tip of the finger. Only clear, natural, or nude-colored nail polish is acceptable while in uniform. Nail decorations are prohibited (e.g., rhinestones).
4. Wigs/weaves/sew-ins - All personnel who so desire may wear a wig/hairpiece providing it conforms to the hairstyle requirements outlined above.

5. Unnatural colors (purple, blue, green, etc.) - are prohibited for male and female officers.

6. Accessories - Beads, butterfly clips, large barrettes, large hair clips or other large hair accessories are prohibited. (Exceptions: bobby pins and hair pins)

12. **EQUIPMENT TO BE CARRIED ON DUTY**

A. Uniform deputies and Sergeants will carry the following while on duty:

1. Expandable Baton (ASP) – Departmentally approved.

2. Handcuffs with key. Brands authorized for department use are: Peerless, Smith & Wesson, Hiatt, American Munitions and ASP.

3. Flashlight – Optional (Stinger in approved holder).

4. Pocket Notebook - bound type or notebook application.

5. Pen and pencil-ballpoint preferred (black or dark blue ink only).

6. Minimum of an additional fully loaded magazine for Glock pistols.

7. Handkerchief (white, clean) - to be used for emergency First Aid.

8. Timepiece- in working condition-a cellular phone may be used as a substitute.

9. Belt - black leather police type, with standard type of chrome buckle. (Sam Browne type belt to be worn with Uniform #3 and #4 only.) Basket weave optional. Nylon may be used but not for formal uniform.

10. Holster - black leather, open type, no flap, with a strap over hammer or back for Glock pistols. Nylon may be used but not for formal uniform.

11. **Authorized firearm** as per Firearms Policy, authorized by the Sheriff, and worn on the dominant hand side with butt facing the rear.

   a. The carrying of a second firearm by any sworn personnel while on duty without the written permission of the Sheriff is prohibited.

12. Identification Cards

   a. Identification Cards will be approved by the Chief Deputy or Sheriff upon appointment or promotion.
1) Identification cards will be issued at City Hall Room 111A; Identification cards are issued Tuesday through Thursday 8:00am to 3:00pm.

2) All personnel are required to have an identification card portrait photo taken in the approved departmental standard attire according to their position.

   i. Civilian personnel – casual business attire
   ii. Sheriff Deputy Sheriff Corporal (proposed). – Blue long sleeve shirt, black tie, badge, name tag, hat with frontispiece and approved Sheriff’s Office pins and medals.
   iii. Sergeant – White long sleeve shirt, black tie, badge, name tag, hat with frontispiece and approved Sheriff’s Office pins and medals.
   iv. Lieutenant and above – White long sleeve shirt, black tie, blouse coat, badge, name tag, city seal lapel pins, rank insignia, and hat with frontispiece.

3) All personnel are required to maintain a current identification card. Outdated photos may be updated at any time if their appearance has changed. This is to ensure an accurate identification of active members of the Office of the Sheriff.

4) Physical inspection of the Office of the Sheriff identification card will be conducted by a Supervisor on a monthly basis. If the employee does not possess a current card, the Supervisor will instruct the employee to report to City Hall Room 111a for issuance of a replacement identification card.

5) All identification cards are required to have an expiration date. All personnel must maintain a current identification card with accurate information. Personnel with identification cards approaching the expiration date may begin the process 60 days prior to the expiration date.

6) Identification Cards will be worn by all personnel in civilian clothes unless they are in an undercover assignment.

b. Official Office of the Sheriff Identification Cards are as follows:

   1) Sergeant to Sheriff-Gold Border
   2) Deputy Sheriff-Blue Border
   3) Deputy Sheriff Officer-White Border
   4) Civilian Staff-Red Border
   5) Civilian Employee-Navy Border

**NOTE:** The expiration date is on the front of card below the badge. The date that photograph was taken is on back of the card.

c. Sheriff ACT 2-114 Certification Card:

   1) Physical inspection of the PCCD card will be conducted by a supervisor on a monthly basis.
2) If the sworn employee does not possess a current certification card, the supervisor will contact the Chief of Staff in order to determine if the certification card has expired

d. Equipment to be carried while Off-Duty

1) Deputy Badge
2) Identification Card
3) Pennsylvania Commission on Crime and Delinquency (PCCD) Act II-2014 Certification Card
4) Firearm (optional)

13. ON DUTY-UNIFORM MAINTENANCE

A. All sworn employees are responsible for the proper care, security, and authorized use of their uniforms and equipment.

B. Replacement or Repair of Badge/Frontispiece

1. When a badge/frontispiece is lost or stolen, the deputy will:

   a. Report the incident to the district of occurrence.
   b. Prepare a memorandum in triplicate to their Deputy Chief stating thereon:

      1) The manner the badge/frontispiece was lost or stolen (include DC#, or incident number when out of jurisdiction).
      2) Request for a temporary badge/frontispiece.

         i. Submit a memorandum to the Deputy Chief for approval. Copy to be retained by submitting officer.
         ii. Submit a memorandum to the Deputy Chief-Internal Affairs.
         iii. Report to Chief of Staff with the original copy of approved memorandum.

   NOTE: When a temporary badge/frontispiece is issued, it is for appearance only. The deputy must use their assigned payroll number on all reports.

2. The Internal Affairs Deputy Chief will obtain from the detective division/jurisdiction of occurrence a copy of the investigative reports detailing the lost or theft of the badge/frontispiece and interview the deputy concerning the circumstances. If it is determined that the loss or theft is due to carelessness or negligence, a memorandum will be sent to the Undersheriff-Finance to arrange for payment.

3. When a deputy’s badge/frontispiece needs repair, they will:

   a. Prepare a memorandum in duplicate to their Deputy Chief outlining how the badge/frontispiece was damaged and request that it be repaired.
b. Submit a memorandum to their Captain/Commanding Officer for approval. Copy to be retained by submitting deputy.

c. Report to the Chief of Staff with the original copy of approved memorandum.

C. Replacement of Lost or Stolen Department-Issued Equipment (Handcuffs, Helmets, Radios, BWCs, and Act II 2014 Cards)

1. All lost or stolen department-issued equipment will be reported to the district/jurisdiction of occurrence (normal reporting procedure is to be followed).

2. The deputy will:

   a. Prepare a memorandum in triplicate to their Deputy Chief, fully explaining the circumstances.

   b. After the Deputy Chief reviews and approves the memorandum, report to 100 S. Broad Street-Land Title Building, with a copy of the approved memorandum to obtain replacement helmet or handcuffs.

   c. The Chief of Staff will:

      1) Receive, review, and approve the reporting officer's memorandum and permit the deputy to obtain replacement handcuffs or helmet.

      2) Obtain from the Detective Division/Outside Jurisdiction assigned a copy of the investigative reports concerning the loss or theft of equipment and interview the officer regarding the circumstances surrounding the loss or theft.

      3) Distribution of Memorandum:

         i. Original -- For helmets and handcuffs to the Chief of Staff.

         ii. For ACT 2-114 Cards to the Deputy Chief of the Training Bureau with a copy of the initial police report.

         iii. Copy -- Retained in Unit File by immediate supervisor.

D. Replacement of Lost or Stolen Department issued cell phones, laptops, or data storage capable devices.

1. All Office of the Sheriff personnel who are assigned city-owned cell phones, laptops or data storage capable devices must immediately report any loss or theft of that Sheriff Office-owned cellular device. Reports will be made immediately to the Innovation and Technology Director via cell at (215) 771-2744 or (888) 608-6111. The IT-Help Desk is staffed 24 hours a day, seven (7) days a week. Once the device is reported it will be deactivated.

2. Deputy Chiefs will ensure the stolen device is also reported to the Detective Division/Jurisdiction of occurrence. The Internal Affairs Deputy Chief shall
investigate the circumstances surrounding all lost devices. Personnel will be guided by the reporting process for lost or stolen equipment as outlined in this Directive.

3. Additionally, all cell phones, laptops, data storage capable devices or cellular devices that are reported lost or stolen must be reported to Innovation and Technology Director via cell (215) 771-2744 or (888) 608-6111. An administrative analysis of the circumstances relating to the loss shall be made and the IT Director will be responsible for issuing replacement city issued cell phones, laptops, or data storage capable devices.

E. When an investigation reveals negligence or carelessness, the deputy will be subjected to disciplinary action and/or be required to pay for the lost or stolen badge, frontispiece, handcuffs, helmet, radio or BWC.

F. Replacement or Repair of Uniforms Damaged in the Performance of Duty:

1. Uniforms/equipment damaged in the performance of duty will be replaced or repaired by the Office when prior to the damage the uniform clothing would normally pass inspection.

2. The deputy will prepare a memorandum in triplicate to their Deputy Chief and state thereon:
   a. Full description of damaged clothing and date it was purchased.
   b. Summary of the incident and manner the uniform was damaged.

3. The Deputy Chief will approve the deputy’s memorandum only when, in their opinion, the request for repair or replacement is valid and state thereon:
   a. damage occurred in the line of duty.
   b. clothing in question would normally pass inspection.
   c. that the incident has been investigated and the facts as stated are true.

4. The Deputy Chief will forward original and first copy of memorandum, along with damaged clothing (through the chain of command) to the Undersheriff-Finance Office.
   a. Copy will be returned to submitting deputy.

5. When request for replacement is approved:
   a. The Undersheriff will send a memorandum to the requesting deputy to go to designated place where clothing will be replaced or compensated.

6. When request for repair is approved:
   a. The Undersheriff will notify deputy to pick up uniform for repair.
b. Deputy will take uniform to designated manufacturer for repair.

7. When request for repair or replacement is disapproved, the Undersheriff (or designee) will notify the deputy to reclaim uniform.

G. Replacement of Leather Coats:

1. All requests for replacement of leather coats, due to damage, will be rejected.

H. Replacement of Identification Cards.

1. Lost Identification Cards:

   a. Deputies will prepare a memorandum in triplicate and submit the original and a copy through their chain of command to the Chief of Staff, requesting a new identification card. The submitting deputy will retain a copy. Include a brief explanation of the circumstances concerning the lost or stolen card and a copy of the applicable police report.

   b. Chief of Staff: Will approve the request and forward it back to the requesting deputy.

   c. Upon receipt of the approved memo, the deputy will take the memo to the Undersheriff-Finance, 100 S. Broad Street – 5th Floor-Land Title Building, to the reception desk and pay the replacement fee. Then proceed to City Hall Room 111– with an approved memo and receipt from Finance.

   d. If the lost identification card is within a year of expiration, the deputy should be in full uniform prepared to have a new updated photo taken.

2. Stolen Identification Cards:

   a. Deputies will prepare a memorandum in triplicate and submit the original and a copy through their chain to the Chief of Staff, requesting a new identification card. Submitting deputy will retain a copy. Include a brief explanation of the circumstances concerning the lost or stolen card and a copy of the applicable police report.

   b. Chief of Staff: Will approve the request and schedule the deputy to appear at City Hall 111 for the new identification card.

   c. If the stolen identification card is within a year of expiration, the officer should be in full uniform prepared to have a new updated photo taken.

   d. All Supervisors will ensure the circumstances concerning the replacement of identification cards are investigated to ensure they are reasonable. The integrity of
the identification card is maintained by the ability to limit the number of cards issued to an individual.

3. Damaged or Expired cards:
   a. No memorandum is needed when returning the damaged or expired identification cards. Personnel should report to the City Hall, Room 111.
   b. Deputies should be in full uniform prepared to have a new updated photo taken.
   c. Identification cards are issued by the City Hall, Room 111. Identification cards are issued Tuesday through Thursday 8:30a.m. to 3:00p.m. Supervisors and employees may contact City Hall 111 for assistance or any questions.

14. LOST/STOLEN FIREARMS

A. All sworn employees are responsible for the proper care, security, and maintenance of their issued firearm and ammunition.

B. Deputies are reminded that carelessness (or negligence) on the part of a deputy facilitating the loss of a firearm, whether privately owned or issued, will be subject to disciplinary action.

C. Replacement of a Firearm

1. When a firearm is lost or stolen, the deputy will:
   a. Immediately Report the incident to the district of occurrence or jurisdiction of occurrence.
   b. Prepare a memorandum in triplicate to their Deputy Chief stating thereon:
      1) The manner the firearm was lost or stolen (include DC#, or incident number when out of jurisdiction).
      2) Request for a temporary / replacement firearm.
         i. Submit a memorandum to the Deputy Chief for approval. Copy to be retained by submitting deputy.
         ii. The applicable Deputy Chief shall prepare a memorandum indicating how the deputy could have prevented the theft/loss from happening.
         iii. Submit a memorandum to the Deputy Chief-Internal Affairs.
         iv. Report to Chief of Staff with the original copy of approved memorandum.
         v. Report to the Armory, where, if approved, the Firearms Technician shall issue a temporary replacement firearm.
2. When a temporary firearm is issued, the Firearms Technician will ensure the serial number of the new firearm is added to the training record of the deputy to memorialize the issuance of the replacement weapon. This will occur in addition to the lost firearm, which will remain in the training record of the deputy, for chain of custody issued if recovered/found.

3. The Internal Affairs Deputy Chief will obtain from the detective division/jurisdiction of occurrence a copy of the investigative reports detailing the lost or theft of the firearm and ammunition and interview the deputy concerning the circumstances. If it is determined that the loss or theft is due to carelessness or negligence, a memorandum will be sent to the Undersheriff-Finance to arrange for a reimbursement payment from the deputy.

15. CLOTHING/MAINTENANCE ALLOWANCE

A. A clothing allowance, as well as uniform maintenance allowance, is allotted to each sworn member of the Office of the Sheriff. All sworn employees assigned to full duty on the date the checks are issued are entitled to the annual uniform maintenance allowance payment. Deputies not on full duty will not receive clothing/maintenance checks unless they return to full duty prior to the end of the fiscal year. Upon return, deputies will submit a memo approved by their respective Deputy Chief addressed to the Undersheriff.

B. It will be the responsibility of the individual deputy to purchase and maintain the required uniforms and equipment as specified in this Directive.

16. RETURN OF EQUIPMENT

A. At the termination of a deputy’s employment, the applicable Deputy Chief will reclaim all Sheriff Office-owned equipment and:

1. Withhold the deputy’s last paycheck until the return of this equipment.

B. The applicable Deputy Chief will ensure all equipment is returned as follows:

1. Armory, Firearms Technician-Training Unit-Office of the Sheriff owned weapon, magazines, black box, and trigger lock.

2. Training Unit Captain -- Helmet, protective vest, and handcuffs.

3. Chief of Staff -- ID card, Act II 2014 card, parking permit, vehicle and keys, and frontispiece. On retirement, deputy sheriffs are permitted to exchange their assigned badge for a Retired Deputy Sheriff badge and retired deputy sheriff ID card.

4. IT Director-Android, iPhone, Blackberry, laptop, etc., if issued.
17. **REPAIR OR REPLACEMENT OF PERSONALLY OWNED PROPERTY DAMAGED IN THE LINE OF DUTY**

A. Claims for the repair or replacement of personal property (e.g., eyeglasses and dentures) damaged in the line of duty must be substantiated by the deputy and authenticated by the immediate supervisor and Captain.

1. If the Captain’s investigation indicates that the damage occurred through negligence or carelessness on the part of the deputy, the claim will not be paid.

B. The deputy must report to their immediate supervisor with the damaged item prior to reporting off duty on the day of the incident.

C. The deputy must prepare a typewritten memorandum in triplicate to the Captain. The memorandum will include:

1. Deputy’s name, payroll number and badge number.

2. Date and time of the incident.

3. Location of occurrence.

4. A brief description of the incident.

5. District Control Number (DC#) or jurisdictional report number.

6. Name, age, and address of offender, if known and when appropriate,
   
   a. If the offender was arrested, list charges and place of hearing.

7. Any injuries sustained.
   
   a. If the deputy is injured, a copy of the Injured Employee Report will be attached to the memorandum.

8. Witnesses to the incident (sworn and civilian), including the addresses of civilian witnesses.

9. Description of item, damage, value, and date purchased.

10. State that no remuneration for the article has been or will be accepted, other than that provided by the Office of the Sheriff.
   
   a. When an offender, or other party, i.e., Victim’s Assistance, offers to pay for the damaged article(s), the individual will be directed to:
1) prepare a check payable to "City of Philadelphia Office of the Sheriff"
2) write a letter of explanation.
3) mail both to the Undersheriff, 5th Floor, Land Title Building, 100 S. Broad Street.

b. Any request resulting in a double payment shall be referred to the Internal Affairs Division for investigation.

11. Attach bills for repair/replacement to the memorandum.

D. The deputy’s supervisor will examine the item in question and note the damage (i.e., left lens broken, frame broken, etc.). In addition, the supervisor will investigate the incident and:

1. Prepare a typewritten memorandum in triplicate to the applicable Captain indicating the results of the investigation and the reasons for approval or disapproval of the deputy's request.

2. Submit the memorandum to the Captain for review.

E. The Captain will approve or disapprove the request and state on the deputy’s memorandum the reason, therefore. Distribute the memoranda as follows:

1. Original & Copy – Training Deputy Chief

2. Copy - Returned to the deputy.

F. The Training Deputy Chief will review the deputy's claim and approve or disapprove the request.

1. When the claim is approved, determine the amount of the Office’s liability, and forward the memorandum to the Undersheriff.

2. When the claim is disapproved, state the reason on the deputy’s memorandum and return to the requesting deputy through the chain of command.

G. The Undersheriff or designee will contact the deputy's Captain and request that the deputy report to Finance, to arrange for payment for the damaged item.

18. LOCKERS

A. The Philadelphia Office of the Sheriff maintains lockers at most of its facilities for the exclusive use of its employees, as a convenience for them and as such, certain responsibilities and restrictions are placed on their use.
B. All Department personnel are hereby placed on notice that the Philadelphia Office of the Sheriff reserves the right to inspect, inventory, view or otherwise search any property owned by the Philadelphia Office of the Sheriff (or City) at anytime. This shall include, but is not limited to lockers, desks, cabinets, and vehicles. Accordingly, personnel should NOT assume any reasonable expectation of privacy in these areas whether locked or unlocked.

C. The individual officer assigned a locker shall:

1. Provide their Captain with a duplicate key or combination for the lock used to secure their locker. (This will facilitate inspections by command personnel.) If a combination lock is supplied for the deputy’s use, only that lock will be placed on the locker.

2. Keep their locker clean and orderly as possible.

D. The individual deputy assigned a locker shall not keep any articles of evidence, confiscated materials, surrendered weapons or firearms, contraband, intoxicants, food or surplus quantities of City or Office forms in their locker at any time. Ensure no adhesive stickers, labels, etc., are placed on any part of the locker.

E. The individual deputy assigned a locker may store the following items in same:

1. All required deputy sheriff equipment as indicated in this directive.

2. Civilian clothes and athletic equipment.

3. Toiletries

4. Off-duty firearm

F. Captains shall conduct monthly inspections of all lockers assigned to personnel under their command. This authority may, in specific instances, be delegated to subordinate supervisory personnel.

19. **SOFT BODY ARMOR**

A. **POLICY**

1. All sworn personnel on-duty and performing a sworn function, will wear their Sheriff Office-issued ballistic/protective vest, unless exempted as follows:

   a. Undercover or detailed to investigative units
   b. Administrative personnel

B. **PROCEDURE**
1. Approved equipment:

   a. Elbeco V1 Poplin External Vest Carrier Style #V1710 (white) and #V1713 (blue)
      
      i. Uniform shirt poplin construction.
      ii. Executive design matches uniform shirt in both style and color.
      iii. Color powder blue or white, consistent with rank.
      iv. Two (2) front pad and pen breast pockets with hidden Velcro closure.

   b. Blauer Armor Skin Style # 8770-1 color #46-blue/color #26-whiteBlauer L/S Street shirt Style #8771-1 color #46-blue/color #26-whiteBlauer S/S Street shirt Style #8772-1 color #46-blue/color #26-whiteBlauer Suspenders Style #174 color #11

   c. Blauer Armor Skin is an armor integration uniform system.
      
      i. This system consists of the Armor Skin vest which covers your existing carrier.

   d. A Street shirt-performance uniform shirt-worn as a base layer or as an alternate uniform shirt.

   e. An optional duty belt suspension system integrated into the vest.

      NOTE: The quilted blue outer carrier for the ballistic panels may only be worn with either the patrol jacket, blouse coat or leather jacket. The quilted outer carrier may not be used while wearing Uniforms #1 or #2.

2. Inspection

   a. All supervisors will inspect their personnel during daily roll call to ensure personnel are wearing the protective vest as required. During this inspection, it is incumbent on the officer to take appropriate action to demonstrate that the ballistic panels of the vest are in place. Such action may include the following:
      
      i. Carefully raising, removing, or unbuttoning the top garment so as to expose the vest to visual inspection, or
      ii. Lightly patting on the front and rear of the vest so as to produce a sound, or
      iii. any other reasonable manner, which will indicate to the patrol supervisor that the vest is being worn.

   b. The supervisor is responsible to ensure that the inspection is notated in pre-planned high-risk incidents; the supervisor will ensure the wearing of body
armor by personnel involved in the incident will be documented on the pertinent report.

c. Deputy Chiefs via the assigned Captain will be responsible for conducting an annual inspection in August of each year.

d. All Deputy Chiefs will ensure that soft body armor assigned to each officer under their command is inspected for the following:

   i. Wear-Damage-Abuse-Misuse -- The "Coolmax" and poly cotton carrier and the ballistic panels they contain will be examined to ensure that excessive wear or other damage has not made the vest unusable. Examples would include damage such as holes, rips, tears, fraying seams, unraveling stitching and severe bunching of the inner material and discoloration.

   ii. Personal Fit -- If during the annual inspection or at any time it is determined that armor no longer meets the standard for proper fit, it will be replaced as soon as possible.

   e. Personnel requiring a replacement vest due to loss, damage or theft will report to the Training Division a memo approved by their Captain and the damaged vest. No memo will be necessary if the replacement is for fit only.

   f. Seams and/or binding will not be opened for any of these inspections.

   g. Panels will be inspected by opening the Velcro sealers on the carrier and visually examining the panels during the Deputy Chief's annual inspection.

C. ANNUAL BODY ARMOR INSPECTION REPORT

1. Every Deputy Chief will be required to submit an annual body armor inspection report. This report will list all body armor, which has been determined as requiring replacement through inspection. It will also include the captain's determination as to normal wear, abuse, or misuse. This annual report will be sent to the Chief of Staff no later than the first Monday after the 15th of September of each year.

D. EMERGENCY REPLACEMENT

1. In the event a vest is lost or stolen, it must be reported immediately through normal procedures for lost or stolen City property.

2. If lost, stolen or damaged, replacement will be obtained by following the procedure indicated in this directive.
3. Vests, which have been shot, punctured, or damaged, must be replaced before the deputy returns to field duty.

E. OFFICERS WITHOUT BODY ARMOR

1. If armor is lost, stolen, or damaged, deputies will be permitted to work in non-field assignments until the vest is replaced.

2. If armor is lost, stolen, or damaged through personal neglect, misuse, or abuse, personnel will be responsible for restitution and subject to disciplinary action.

3. Deputies who have forgotten their armor will be carried vacation/holiday or leave without pay until they return to work with the required equipment and may be subject to disciplinary action.

F. CARE AND MAINTENANCE

1. Each deputy who has been issued soft body armor will be responsible for its routine care in accordance with the manufacturer's direction.

2. Instructions for proper care are attached to the vest.
   
   i. NEVER EXPOSE TO DIRECT SUNLIGHT  
   ii. NEVER DRY CLEAN  
   iii. NEVER USE BLEACH  
   iv. NEVER PUT BALLISTIC PANELS IN THE WASHING MACHINE

3. Under no circumstances is a deputy to attempt to mend or repair soft body armor. If any mending or repairs are needed; the deputy will follow the procedures outlined in this directive for replacement.

G. STORAGE

1. Sheriff Office-owned protective vests will not be kept in vehicles. (Exception: personnel in “on-call” status will be permitted to store their vests securely in their vehicle only for that period they remain in on-call status.)

2. Ballistic panels should be stored flat, not folded.

H. REPORTS OF "SAVES"

1. Whenever soft body armor saves a deputy, whether as a consequence of gunfire, blunt trauma, vehicle accident, fall or any other instance where the armor saved the deputy, a report from the deputy's Captain will be forwarded to the Deputy Chief-Training Bureau, through proper channels within 10 days of the incident. This report will include the DC#, Investigative Control# and copies of the investigation reports.
2. The body armor manufactured from Kevlar is vulnerable to attack by knife or other
sharp instrument, such as an ice pick. However, it is likely to lessen the severity of
injuries from a slashing attack.

20. S.O. BICYCLE PATROL

A. POLICY

1. All personnel assigned to Bicycle Patrol will maintain the prescribed uniform as well
   as any items distinctive to their assignment.

2. The Training Division will retain responsibility for training.

3. The Deputy Chief of Uniformed Services will have sole responsibility for the
   assignment of these deputies.

4. No uniform or equipment other than that described herein will be permitted while in a
   uniform bicycle patrol assignment.

5. Deputies will wear the uniform of the day when not assigned to bicycle patrol.

B. PRESCRIBED UNIFORM

1. Uniform bicycle patrol deputies will comply with the below listed prescribed uniforms
   and equipment. All uniforms and equipment will be available for inspection. No
   substitutions will be permitted.

   a. Winter Uniform:

      1) One (1) head cover (solid navy or black knitted material)
      2) One (1) winter cycling vest with bolero (Ultrack), yellow and navy
      3) One (1) pair cycling pants (Ultrack) navy
      4) One (1) pair cycling pants (Supplex) navy
      5) One (1) pair insulated high-top boots, black
      6) Three (3) navy colored sweatshirts
      7) One (1) pair winter riding gloves (solid black or navy only, no ski gloves)
      8) Three (3) black or navy-colored turtleneck shirts with PSO logo

   b. Summer Uniform:

      1) Two (2) pair summer shorts (Supplex), navy
      2) Three (3) light blue short-sleeve staff shirts, including silk-screened badge and
         nameplate.
      3) Three (3) pair socks (Kevlar optional) solid color, white or navy mid-calf
      4) One (1) pair black leather cross-training sneaker (high top)
      5) One (1) pair summer riding gloves
6) One (1) clear plastic raincoat

c. Duty Holster and Related Equipment:

1) One (1) nylon web belt, black
2) One (1) nylon web holster, black
3) One (1) nylon web handcuff case, black
4) One (1) nylon web speed loader/magazine holder, black
5) One (1) nylon web baton loop

d. Mountain Bike and Related Equipment:

1) One (1) Raleigh Police mountain bike (Other bikes purchased before the effective date of this directive AND previously approved will be approved. Any bikes purchased after the effective date of this directive will be as stated or departmentally approved by the Sheriff.
2) One (1) cargo trunk, black nylon type, waterproof preferred
3) One (1) Kryptonite lock (optional)
4) One (1) Advocet computer (optional)
5) One (1) water bottle and water bottle cage
6) One (1) Nicelit front light (other lights optional if approved)
7) One (1) mirror
8) One (1) helmet, bell image, white ONLY, with Office approved decals and insignia
9) Two (2) pair eye protection, tinted and clear
10) One (1) baseball hat with PSO emblem, navy

e. All bicycles acquired become Sheriff’s Office property, and as such, will require property numbers.

f. All other provisions of this directive (where appropriate) will apply and be strictly adhered to.

g. This is a community-funded program. The Captain will ensure strict accountability for any funds solicited and/or disbursed.

C. REGULATION UNIFORMS

1. Regulation Uniform #1

   a. Supplex cycling shorts; short-sleeve light blue staff shirt; black cross-training sneakers with socks, mid-calf, solid colored white, or navy

2. Regulation Uniform #2
a. Supplex cycling pants; short-sleeve light blue staff shirt; black cross-training sneakers with socks, mid-calf, solid colored white, or navy

3. Regulation Uniform #3

a. Supplex cycling pants; long sleeve navy blue sweatshirt; cycling vest with optional bolero (Ultre or Supplex); black cross-training sneakers or black high-top boots (optional).

4. Regulation Uniform #4

a. Ultre cycling pants; long sleeve navy blue sweatshirt and/or black or navy PSO turtleneck; Ultre cycling vest and bolero; black high-top boots; winter riding gloves; head cover.

5. Lieutenants and above may substitute white shirts in place of blue in all sections.

D. Sheriff Office-approved bicycle helmets will be worn with all the above uniforms and whenever operating a bicycle. Baseball caps may be worn as cover when deputy is not operating their bicycle.

BY ORDER OF:

[Signature]

SHERIFF      DATE

82
OFFICE OF THE SHERIFF
CITY AND COUNTY OF PHILADELPHIA

Date: February 24, 2021
Subject: Beards and Goatees Policy

Purpose: To outline the rules and procedures regarding the wearing of Beards and Goatees while on duty.

1. Beards and Goatees are not permitted except when consistent with assignment.

Exceptions:
A. Medical Exception – A beard may be worn for health reasons when a waiver is authorized by the Safety Office based upon the advice of the City’s Medical Director that the employee had a medical condition that prevents him from shaving. If a waiver is authorized, facial hair will be kept trimmed and neat, not to exceed ¼” in length. Individuals granted a waiver shall be monitored and reviewed by the Medical Director every three (3) months to determine if the medical condition persists to warrant the continuation of the waiver.

B. Religious Exception – A beard may be worn when a waiver is authorized by the Sheriff. Religious Beard waivers are granted as a courtesy only. Once submission of a memo and proper documentation from his religious representative stating the individual named does practice said religion. Consideration will be made to grant or deny the waiver by the Sheriff. The request for a waiver must have the name of the religion, the specific beard requirement and must be on the religious institution’s letterhead. The documentation must be notarized or subject to verification. If a waiver is authorized, facial hair will be kept trimmed and neat, not to exceed ¼” in length. Waivers will expire after 6 months and employees must reapply at the end of each term.

Approved/Denied

[Signature]
Sheriff Rochelle Bilal

2-24-21

83
DIRECTIVE: #5
SUBJECT: TELEPHONE PROCEDURES
ISSUED DATE: 05-11-2020
REVISED: 02-24-2021

1) PURPOSE:

The purpose of this Directive is to establish a policy on Telephone Procedures for members of the Philadelphia Sheriff’s Office. The first contact many residents have with the Sheriff’s Office is with the voice that answers the telephone when they call us. Courtesy, professionalism, and empathy go a long way towards cultivating positive impressions of the Sheriff’s Office and promoting public service among the employees.

2) POLICY:

A. All Sheriff’s Office employees shall conform to the following policy:

1. All Sheriff’s Office employees shall be courteous and professional, while attempting service callers by:

   a. Answering the telephone promptly when it rings. The telephone should be allowed to ring more than three (3) times.
   b. Identifying oneself and the particular unit/division called when making or receiving a call.
   c. Speaking distinctly and clearly into the transmitter using an even toned, friendly and natural voice.
   d. Addressing the caller properly (use the caller’s title if it is known. If not, sir or ma’am).
   e. Actively listening to issue raised by the caller; indicated by communicating that you understand or require clarification of the issue.
f. Trying to be helpful and furnishing the caller with the correct information. If the employee does not know the answer, she/he will inform the caller of her/his lack of knowledge and immediately contact the unit’s supervisor for the right answer. It shall be noted that only general and public information shall be released to the public by front line staff. For more complicated matters or issues involving specific legal questions or complaint against an employee shall be forwarded to a supervisor within the unit. The supervisor shall determine if the matter will be handled within the unit, transferred to another unit, or forwarded to the Undersheriff or to the Internal Affairs Division. In all cases, all Sheriff’s Office staff shall complete either a Philadelphia Sheriff’s Office Complaint Form or Constituent Services Form.

g. Transferring calls immediately; explaining why, to whom the caller is being transferred and the extension the caller is being transferred to. To transfer a call, use the transfer button on your land line, dial the number you’re transferring the caller to and then hang up.

2. The employee shall also keep a pad and pen available.

   a. Document the caller name and call-back number in the event of a disconnection.
   b. The employee shall immediately return any unintentionally disconnected call.
   c. Employees shall never intentionally disconnect calls. Discourteous calls shall be forwarded to the unit supervisor for disposition.

3. Follow up calls promptly and relay results back to caller.

4. Apologize for any interruptions/delays, remain customer focused and engaged and close each call professionally.

   a. During an extended delay (over 5 minutes), periodically inform caller of status.
   b. Conclude calls on pleasant note, if possible.

5. **Document**: The employees answering the telephone are responsible for documenting the assistance they provide callers on the Constituent Service Form or Complaint Form. This rule applies to all calls including calls from other Law Enforcement Agencies and governmental jurisdictions as
official business has been conducted and the documentation provides an accurate assessment and written record of the scope of services provided by this office.

B. All Sheriff’s Office employees shall conform to this directive immediately.

1. This directive supersedes all other Telephone Communication Policies.
2. This directive is effective immediately.

BY ORDER OF:

[Signature]
SHERIFF
DATE 2-24-21
I. PURPOSE:

A. The purpose of this directive is to establish a policy on Memorandum/Report Writing for members of the Philadelphia Sheriff’s Office.

II. POLICY:

A. Deputies/employees serving in the Philadelphia Sheriff’s Office shall conform to the following policy:

1. There are three (3) memorandum forms used by the Philadelphia Sheriff’s Office. The 82-S-1 (8W’ x 11” – long form), 82-S-1A (8W’ x 7” – short form), and memorandums formatted for email distribution.

2. The opening paragraph(s) should contain a brief synopsis indicating the general content of the report. They should also include such information as dates, times, locations, persons involved, etc., so that anyone reading the report can intelligently evaluate and understand the (who, what, when, where, and why) of the report.

3. The succeeding paragraphs shall make up the body of the report and must be composed in a logical sequence. Adequate attention should be given to the chronological order of events and care must be exercised to ensure that all available information is included.

4. The answers to the question – WHO, WHERE, WHY, WHAT, WHEN, AND HOW must be given. If it is necessary for the recipient of the report to request additional information, the report is considered incomplete.
5. Care must be given to use proper sentence construction, correct spelling, and correct format. Outlining a report prior to writing it often times helps the writer avoid unintentional omissions and clarifies the materials presented.

6. There is no rule that states reports must be confined to a single page.

III. PROCEDURE:

A. Addressing the Memorandum/Report

1. TO: The person who requested that you submit the report or the person to whom you direct the report.

2. For the sake of uniformity, when you address a communication to a person who commands a Unit/Division, you will write, or type as follows:

   a. RANK, TITLE, FULL NAME

3. The supervisor who reviews and approves the report shall place his/her signature below the signature block.
DIRECTIVE:  #7  
SUBJECT:  HANDLING OF PRISONERS  
ISSUE DATE:  05-13-2020  
REVISED DATE:  02-24-2021

I. PURPOSE:

A. The purpose of this directive is to establish a policy on the Handling of Prisoners by members of the Philadelphia Sheriff’s Office.

II. POLICY:

A. Deputy Sheriffs shall conform to the following policy:

1. The Deputy Chief of Criminal Operations shall implement standard operating procedures (SOPs) to ensure the safety of the public, Sheriff Office personnel, and all prisoners.

2. The Detention Unit Captain, or designee, shall ensure that no prisoner is released from the Sheriff’s Office custody unless authorized by court order.

   a. Court ordered release documents shall be signed and securely emailed or faxed to the Philadelphia Prison, and only if authorized by the Philadelphia Prison by secure return fax or email, may the prisoner be released.

   b. A copy of the court order and the prison release authorization shall be printed and attached to the tracking office paperwork for that day that encompasses all prisoners released from the Detention Unit.

3. The Detention Unit Captain or designee shall ensure that deputies maintain the maximum level of control over prisoners in Philadelphia Sheriff’s Office custody, at all times.

4. Deputy Sheriffs shall search every prisoner prior to accepting custody to ensure his/her safety and the safety of others.
III. PROCEDURE:

A. Deputy Sheriffs searching prisoners shall:

1. Before searching a prisoner inquire whether he/she possesses any sharp objects.

2. Instruct prisoners to empty his/her pockets.

3. Always conduct a search of prisoners and their effects wearing personal protective equipment (PPEs), i.e. shields, facemasks, disposable nitrile gloves, social distancing, etc.

4. The search shall include removal and physical inspection of shoes or boots, checking cuffs, waistbands, hems, belts, coats, hair, wigs, mouth, and legal work and then thoroughly patting down the person being searched. A search of persons with physical disabilities shall include all devices, aids, crutches, canes, wheelchairs, walkers, and metal detector/scanner.

5. A deputy shall not search a prisoner of the opposite sex unless exigent circumstances exist. In those extreme cases a deputy may conduct a limited search with a hand-held detector/scanner.

6. A deputy shall have another deputy present when he/she searches/restraints a prisoner.

7. A deputy shall neither provide nor permit any prisoner to possess any instrument or object which is or could be considered to be a weapon or instrument of escape.

B. Except during transport, prisoners shall be restrained with their hands cuffed behind their back with their thumbs pointed downwards. If a belly chain is used, the prisoner shall be cuffed with his/her hands in the front of his/her belly.

C. A deputy using an elevator while escorting a prisoner shall position the prisoner by having him/her face the rear wall and distance themselves to impede exit via the elevator door.

D. Juveniles prisoners:

1. Shall be restrained consistent with Rule 139, Use of Restraints on the Juvenile. Restraints shall be removed prior to the commencement of court proceedings unless the judge determines, on the record, and after providing the juvenile an opportunity to be heard, that restraints are necessary to prevent:
a. Physical harm to the juvenile or other persons.
b. Disruptive courtroom behavior, evidenced by a history of behavior that created a potentially harmful situation or presented substantial risk or physical harm, or
c. If a juvenile reveals high risk/escape potential or other relevant factors, from fleeing.

2. This rule only applies to all juveniles charged in Family Court. It does not apply to certified juveniles who are charged in adult criminal court.

3. This rule does not preclude the use of restraints on juveniles during transport. Juveniles shall be restrained during transport.

4. A deputy shall neither provide nor permit any juvenile prisoner to possess any instrument or object which is or could be considered to be a weapon or instrument for escape.
Philadelphia Sheriff's Office

DIRECTIVE: #8
SUBJECT: MOBILE PRISONER TRANSPORT
ISSUE DATE: 05-13-2020
REVISED DATE: 02-24-2021

I. PURPOSE:

A. The purpose of this Directive is to establish a policy on the prisoner transport when performed by members of the Philadelphia Sheriff's Office.

II. POLICY:

A. All Philadelphia Sheriff's Office sworn staff shall conform to the following policy.

   A. The Transportation Captain, or designee, shall:

      a. Be responsible for the transportation of prisoners.
      b. Shall implement prisoner transportation procedures that ensure the safety of the public, transporting deputies, and prisoners.
      c. Shall ensure that transportation activities preserve and safeguard the rights of prisoners to the best of our ability.

   B. Deputies conducting prisoner transport shall:

      i. Dress in the uniform of the day, complete with all required and issued equipment.
      ii. Read and understand all court orders and special instructions and ensure that all required paperwork, including writs and commitments are in presented to them before transporting a prisoner.
      iii. Remove all personal property including bags and medication from a prisoner before transporting him/her, and ensure those items are transferred to the custody of staff at the destination facility.
      iv. Thoroughly search every prisoner prior to transport.
      v. Secure each prisoner with restraints prior to transport.
vi. A deputy shall neither provide nor permit any juvenile or adult prisoner to possess any instrument or object which is or could be considered to be a weapon or instrument for escape.

   a. Juvenile prisoners shall be restrained the same as adults.
   b. Provide special care and consideration to prisoners who are physically handicapped.
   c. Physically disabled or visibly pregnant prisoners shall be restrained only to the extent necessary to prevent them from escaping.
   d. If any prisoner's condition effectively prevents him/her from escaping and the application of mechanical restraints would create an unnecessary and unjustifiable hazard to them that mechanical restraints are not to be used.
   e. Consider the age, condition, background, and the extent of the disability of a physically disable prisoner when determining the level of restraint necessary for the prisoner.

vii. Ensure that the transport vehicle has been searched, inspect and is in operable condition prior to and post transport.

viii. Transport no more than available seats in the transport vehicle.

   a. During times declared a pandemic, or national health crisis, transportation supervisor’s and deputies are responsible for positioning prisoners (at minimum) within recommended Center for Disease Control social distancing guidelines.

ix. No less than three (3) deputies shall be assigned to a bus that is used to transport prisoners; one (1) shall sit in the rear compartment of the bus during the transport. No less than two (2) deputies shall be assigned to the van transporting any prisoner.

x. The deputy driving maintains control and focus upon the operation of the transport vehicle. The assistant driver shall be responsible for recording, operating the radio, and cell phone communications.

xi. Provide meals to prisoners when transportation duties span considerable distances or an extended time periods; typical, in excess of 200 miles or three (3) hours.

   a. A deputy sheriff shall procure meals from a randomly selected fast-food restaurant by utilizing the restaurants drive-thru window.
   b. The prisoner(s) remain inside the vehicle while consuming the food.

xii. Instruct the prisoner(s) to use the bathroom prior to transport.

   a. If the need to use the toilet occurs during a transport, the deputy sheriff shall be responsible for providing toilet facilities for the prisoner.
b. A deputy shall absolutely factor the custody status of the prisoner and the availability of a suitable facility when determining whether to grant the request. Preferred facilities are police and fire stations, local jails, and if unable, highway maintenance facilities, or gas stations with side door restrooms.

1) Selection of the location shall be at random. Do not let the prisoner suggest the location.
2) Park as near to the restroom as possible.
3) Search the restroom for anything that can be used as a weapon or an instrument of escape.
4) Do not remove restraints from the prisoner.
5) Maintain constant physical (hands on) control of the prisoner while he/she is out of vehicle.
6) If the restroom is too small to accommodate the prisoner and the deputy at the same time, the deputy shall position himself/herself in the doorway and afford the prisoner enough privacy to attend to his/her needs, but the door shall not be closed.

xiii. Shall not stop to render emergency aid during a prisoner transport but a deputy shall utilize his/her radio or cell phone to report and to summon aid.

xiv. Shall render any necessary aid, consistent with his/her training, whenever prisoners are not being transported.

xv. A deputy shall take the following actions in the event a prisoner escapes custody.

a. Pursue the prisoner and re-capture him/her.
b. Establish contact with the state, Sheriff, or local police and request assistance.
c. Contact the Transportation Supervisor, or the on-duty supervisor
d. Make no statement to the press, referring any media inquiries to the PIO.
e. Prepare and submit a written report concerning the event to your supervisor prior to end of tour.

xvi. A deputy shall take the following action if a hostage situation develops during the transportation of a prisoner.

a. Implement a plan which is least likely to cause death or serious bodily injury.
b. Attempt to develop a dialog with the prisoner.
c. Summon police assistance.

xvii. If during the transportation detail, a prisoner becomes injured, the transporting deputies shall seek medical treatment for the prisoner.
a. The transporting deputies shall evaluate the prisoners' complainant
and if necessary, shall seek medical treatment for the prisoner.
(Security protocol shall be used).
b. The transporting deputies shall file an incident report.

xviii. If in the course of transport, deputies become aware that they are being
followed, the non-driving deputy shall contact state/local police for
assistance.

a. If for any reason contact cannot be made and help summoned,
continue to travel on the main roadway until you reach a police/fire
station or other government building, hospital, or industrial site where
help may be summoned.

xix. If the transport vehicle develops mechanical trouble during the transport, a
deputy shall:

a. Notify sheriff’s radio or if out of range, contact the local/state police or
sheriff’s office for assistance.

1) If the breakdown occurs within the metropolitan area, your
supervisor will provide the means to continue the transports.
2) If the breakdown occurs outside of the metropolitan area, request
the state/local police or sheriff office to contact the local road
service/towing company for assistance.
3) If it becomes necessary to tow the vehicle or to jack the vehicle up
to change a tire, the prisoners must be removed from the vehicle
prior to towing or jacking up the vehicle.

b. If repairs cannot be made right away, request the local state/local
police or sheriff office to transport your prisoners to the nearest state
prison/county jail. Your primary concern is the security of the
prisoners.
c. A deputy shall promptly notify his/her supervisor of the situation.

xx. If a deputy performing a transport is unable to arrive as scheduled with a
prisoner, he/she shall notify his/her immediate supervisor by
telephone/cell phone and provide new estimated time of arrival.

a. If the immediate supervisor is unavailable or after normal working
hours, then notify the on-duty supervisor at the lobby desk of the
Criminal Justice Center.

xxi. When deputies of the same sex transport prisoner of the opposite sex, they
shall:
a. Notify radio.
b. Record the time of departure and the vehicle's odometer reading.
c. Record the time of arrival and the vehicle's odometer reading.

xxii. The use of multi-media personal entertainment devices, including but not limited to gaming apps, non-business cell calls, music apps or saved music, computers and CD/DVD players are prohibited by deputies while they are on duty.

a. The use of a cell phone is prohibited by any deputy operating a vehicle unless exigent circumstances exist.
b. All necessary cell phone communication, while the vehicle is in motion shall be conducted by the non-driving deputy.
c. While not driving use of a personal phone to access Office of the Sheriff emails or Power DMS training apps in a safe situation are permitted.

BY ORDER OF:

[Signature]

SHERIFF

DATE
III. PURPOSE:

A. The purpose of this Directive is to establish a policy on security in the Detention Unit Areas.

IV. POLICY:

A. Deputies of the Philadelphia Sheriff’s Office shall conform to the following policy:

i. The Commander–Detention Unit, or designee, shall be responsible for the complete and efficient operation of the detention unit including the security of his/her personnel, the prisoners and the physical plant and its related equipment and records.

ii. The Commander–Detention Unit, or designee, shall ensure that all office equipment, metal detectors, power supplies, switches, lights, cell locks, doors, benches, inmate toilets, elevators and fire extinguishers are in proper working order and reports any deficiencies in order to have them corrected, and replenishes first aid supplies as necessary. These objectives shall be realized through the use of the sanitation security report form.

iii. The Commander–Detention Unit, or designee, shall ensure that deputies assigned to the detention unit receive search and seizure training and are proficient in search techniques.

iv. The Commander–Detention Unit, or designee, shall ensure that a thorough search is conducted of the cell room at the beginning of his/her tours of duty BEFORE and AFTER prisoners are placed into any holding area. A thorough search shall include but not limited to:

   a. The floors, walls, ceilings, especially around the light fixtures, the male and female cells, commons areas, aisles and trash receptacles and elevators.
   b. The top and underside of benches and furniture.
c. In, around, under, alongside inmate toilets and floor drains.
d. Openings in cell door tracks, the backs of doors.

b. The Commander—Detention Unit, or designee, shall provide a safe storage area
   for firearms in the sally port of each facility where prisoners are held.
c. The Commander—Detention Unit, or designee, shall ensure that no person (sworn
   or civilian) is permitted entry into the detention unit with a firearm.
d. The Commander—Detention Unit, or designee, shall ensure that it is mandatory
   that anyone who enters the detention unit not employed by the Sheriff’s Office
   signs the daily log. The name, signature, title, organization, nature of the
   individual’s business and time in and time out, department and badge number (if
   applicable) shall be recorded.
e. The Commander—Detention Unit, or designee, shall ensure that a prisoner or
   prisoners who is/are testifying against other prisoner(s) are separated.
f. The Commander—Detention Unit, or designee, shall ensure cell overcrowding
   does not take place and that if overcrowding occurs, it’s brought to the attention
   of the Sheriff or his designee, and rectified by the highest-ranking supervisor in
   the detention unit.
g. Deputies shall open only one (1) door of a multi-prisoner cell in the detention unit
   at a time.

V. PROCEDURE:

A. Accountability: Standardizing Security Procedures

   i. The Commander—Detention Unit, or designee, shall ensure that all
      detention unit keys are accounted for at the beginning and end of the unit’s
      operations, and entries detailing those actions are made in a detention unit
      logbook.

   ii. The Commander—Detention Unit, or designee, shall ensure that the
       detention unit, any cells, visit areas, elevators, and adjacencies are
       searched prior to securing the unit at the end of the unit’s operations, and
       logged into the detention unit logbook.

   iii. The Commander—Detention Unit, or designee, shall ensure that all
        deputies working in a detention unit capacity have reviewed the detention
        unit policies and procedures and acknowledged receipt in electronic policy
        management software.

BY ORDER OF:

[Signature]

SHERIFF

DATE
VI. PURPOSE:

A. The purpose of this Directive is to establish a policy for Uniformed Service Court Safety performed by sworn deputies in the Philadelphia Sheriff’s Office.

VII. POLICY:

A. Deputies in the Philadelphia Sheriff’s Office shall conform to the following policy:

a. The Sheriff, or designee, shall inform president judges in this jurisdiction that Uniformed Services Court Safety deployment and strategies are the sole responsibility of the duly elected Sheriff in the Commonwealth of Pennsylvania. The designated Chief Inspector, Uniformed Services is the primary contact for judicial court safety concerns.

b. When a sensitive situation arises or unusual circumstances are anticipated that create overall safety concerns, more stringent security procedures will be implemented. The Deputy Chief – Uniformed Services or Chief Inspector – Uniformed Services shall work with the presiding judge jointly consider/implement additional screening procedures for persons who wish to enter affected courtroom(s).

VIII. PROCEDURE:

a. The Chief Inspector-Uniform Services will be responsible for the implementation of security screening in all courthouse and city council facilities

a. Each deputy sheriff shall receive a radio with Sheriff/PPD M or T Band access.

b. Every deputy sheriff is assigned a unique call-sign based upon their location served and badge number.
c. Call signs for all deputies are disseminated to deputy sheriffs at roll call and maintained by the desk sergeant and all on duty Philadelphia Sheriff’s Office Uniform Services Supervisors.
d. When additional security screening measures are in place, the walk-through metal detector and physical search protocols shall be implemented and documented by deputy sheriffs.
e. A systematic search of the courtroom shall be conducted daily by assigned deputies.

b. The Chief Inspector – Uniform Services, or designee, shall increase the number of deputies when it is anticipated that multiple defendants will be present in a courtroom, or when other security concerns beget deployment of additional deputies.

c. A Uniform Services Sergeant or above shall assign deputies positions in courtrooms that facilitate the safety of the judge, spectators, and are in close proximity to the defendant(s) to ensure immediate law enforcement intervention should any person become unruly or attempts to assault someone, escape, etc.

d. The Uniform Services Supervisor shall ensure deputies operate within the confines of the laws of search and seizure when inspecting any boxes, bags, and packages that appear inappropriate.

e. Deputies assigned to courtrooms shall pay particular attention to anyone who approaches the judge’s bench without the permission of the judge.

BY ORDER OF:

[Signature]

SHERIFF DATE
Philadephia Sheriff's Office

DIRECTIVE: #11
SUBJECT: PRISONER/DEFENDANT SECURITY
ISSUE DATE: 05-13-2020
REVISED DATE: 02-24-2021

IX. PURPOSE:

A. The purpose of this Directive is to establish a policy on Prisoner/Defendant Security in the courts for the Philadelphia Sheriff's Office.

X. POLICY:

A. A Deputy Sheriff with the Philadelphia Sheriff's Office shall conform to the following policy:

a. The Deputy Chief-Uniform Services, or designee and the presiding judge shall confer in advance to evaluate what additional security measures are required for high risk defendants.

b. Deputy Chief – Uniform Services or designee shall provide the judge with the information relating to the defendant’s security and any options for maintaining maximum control of the defendant during the proceedings, including the use of various restraints.

c. The Chief Inspector – Uniform Services shall be responsible for deputy’s adherence to any guidelines established by the Deputy Chief – Uniform Services and the presiding judge.

XI. PROCEDURE:

A. Deputies shall search each cell of his/her adjacency as well as the prisoner’s side of the attorney booth thoroughly before securing any prisoner into it. Searches will include:

a. The floors, walls, ceilings, especially around the light fixtures, of the male and female cells, common areas aisles and trash receptacles.

b. The top and underside of benches and furniture.

c. In, around, under, alongside inmate toilets and floors drains.
d. Openings in cell door tracks, the bottoms, and the backs of doors.

e. A deputy shall ensure that every prisoner is searched prior to entering the courtroom.

f. A deputy shall use restraints on defendants appearing in post-trial matters as they enter the courtroom; specifically, a restraining belt with handcuffs. Defendants must be handcuffed in front their bodies. The judge may order the restraints removed and will consider each defendant on a case by case basis. The judge may or may not solicit input from the deputy on this matter. A deputy should be prepared to articulate the reasons for the need for the restraints.

g. Information such as the nature of the charges; the fact that the defendant stands before the court convicted; the defendant’s current demeanor and behavior; any statements made by the defendant stating his intention to escape or be disruptive; prison and past history can all be used to support the use of restraints on the defendant. A deputy will comply with the judge’s directives.

h. The Unit Commander, or designee, shall ensure that during multiple defendants’ hearings, each deputy controls no more than one prisoner at a time.

i. When one or more defendants are on trial with a custody defendant, each of the non-custody defendants shall be searched prior to being seated near the custody defendants.

j. Deputies shall always maintain maximum control over a prisoner.

k. Deputies shall take appropriate action in dealing with violent or disruptive defendants.

l. Deputies may search non-custody defendants prior to their hearing.

m. Deputies with prisoners shall use restraints by:
   a. Handcuffing prisoners behind their back and maintaining “HANDS-ON” control of the prisoner.
   b. Additional restraints may be used at the discretion of the deputy with justification and the consent of supervisor.

n. Deputies shall search the adjacency when leaving the courtroom to ensure that all prisoners are returned to central holding. Cell doors shall be left open for the cleaners, but the doors between the adjacency and each courtroom must be closed and locked.
DIRECTIVE:       #12
SUBJECT:         JUDICIAL THREATS/WITNESS PROTECTION
ISSUE DATE:      05-13-2020
REVISED DATE:    02-24-2021

XII. PURPOSE:

A. The purpose of this Directive is to establish a uniform policy for the Philadelphia Sheriff’s Office in the investigation and response to Court/Judicial Threats/Witness Protection duties.

XIII. POLICY:

A. Philadelphia Office of the Sheriff deputies shall conform to the following Witness Protection policy:

a. The Sheriff, or designee, shall be responsible for the protection of witness when directed by the court.
b. The Deputy Chief – Uniform Services, or designee, shall ensure that a Court has drafted and endorsed an order by a Judge for the protection of a witness.
c. All Judicial Orders concerning Prisoner Transportation, Separation, Housing, etc., must be delineated on a Court Order that is signed by the issuing Judge. “Sealed Copies” of the court order will be kept on file by the cell room supervisor for the duration of the trial, or if deemed necessary by the Deputy Chief (Uniformed Services).
d. “Sealed Copies” of the court order shall be forwarded to the following supervisors:
   a. Cell room supervisor
   b. Transportation supervisor
   c. NEPA supervisor
   d. Prisoner Holding Facility
e. The Deputy Chief – Uniform Services or designee, shall ensure all Protection Court Orders/Court Orders are enforced. The Unit Commander shall designate a subordinate supervisor to enter all “Protection Orders” into “CMR” Prisoner Alert Listing Program
f. The Deputy Chief - Uniform Services, or designee, and the Judge shall meet to evaluate the prerequisite level of security required to be provided for a witness, and collaboratively work to draft the specifics in the Court Order accordingly.

g. Security measures shall be based on actual intelligence received by the supervisor, which shall include, but not be limited to the following:

   a. Threats of "intimidation" against the witness.
   b. Threats of "intimidation" against the witness's family.
   c. Previous acts of intimidation.
   d. Police Reports/Prison Reports.
   e. Files and feedback from the District Attorney (ex., a DA’s request for separation).
   f. Deputy observations, arrests, information overheard, video footage, location-based data, or other intelligence gleaned as a result of an incident involving intimidation.
   g. Deputies assigned to all courtrooms, hearings, trials, particularly, "Witness Protection Trials" shall remain alert for video/audio/picture recording of witnesses, and/or acts, reports, of threats made against witnesses, jurors, judges, prisoners, lawyers, law enforcement personnel or any other members of society, when such threats may interfere with the "Judicial Process". Intelligence Units at each facility with liaisons to PPS, PPD, and D.A.’s office shall be established by the Deputy Chief – Uniform Services.

h. Any deputy that witnesses, observes, or is informed of a witness intimidation incident, firsthand shall immediately notify their immediate supervisor. Prompt notification helps to augment witness safety, inform the assigned Assistant District Attorney and Judge, and may result in a hold being placed on the defendant for investigation into possible charges.

   a. Absent exigent circumstances the immediate supervisor shall retrieve and duplicate any video of the incident for evidence preservation and future prosecution.

i. The Uniformed Services Deputy Chief, or designee, shall implement security measures for the protection of the witness.

   b. Any supervisor may initiate "Witness Protection" at any time, from an incident involving two prisoners fighting, issuing a verbal command for a "Separation", or upon receiving an endorsed and approved judicial "Court Order" relating to either a "High Risk", or a "Low Risk" trial.

B. Philadelphia Sheriff's Office deputies shall conform to the following policy on Judicial/Court Threats:
i. The Deputy Chief - Uniform Services shall upon receiving information of a Judicial Threats have the primary responsibility to promptly secure a Judge.
ii. The DC Uniform Services shall also ensure that any employee under his/her command who receives such a complaint forward all information relating to the Judicial Threat Incident via memorandum (and Everbridge) to the Executive Staff and Homeland Security Unit.
iii. The DC Uniform Services, or designee, shall immediately implement security measures for the protection of the Judge/court who was a target of who received threats. This includes personally notifying the Sheriff or Chief Deputy of any staffing needs. The DC Uniform Services or designee shall also notify the:
   a. PSO Homeland Security Unit Commander
   b. Philadelphia Police – Dignitary Protection Unit (685 – 1180/81)
   c. Philadelphia Police – Counterterrorism Bureau

These mandatory notifications should help to immediately provide the appropriate “level of protection necessary” for the Judge/Official and facilitate implementation of an operational plan.
iv. The Warrant Unit Captain shall:
   a. Compile copies of all related incident reports as soon as possible.
   b. Maintain a record of all judicial threats.
   c. Assume the planning function for future protection details after the initial detail date.
   d. Enters all details of the threat event into the Administrative Office of the Pennsylvania’s Courts statewide web site.

BY ORDER OF:

[Signature]

SHERIFF       DATE

105
XIV. PURPOSE:

A. The purpose of this Directive is to establish a uniform policy on procedures used by Office of the Sheriff Deputies when securing High Risk Trials in courts.

XV. POLICY:

A. Deputy Sheriffs shall conform to the following policy:

a. The Chief Inspector - Uniform Services or designee, with incorporated input from the presiding judge, will decide upon the level of security required, and then shall establish a pre-trial operations plan that includes, but is not limited to:

   a. The level of security to be provided for the Judge.
   b. The level of security to be provided for the jury and witnesses.
   c. The level of security to be provided for the prisoner.
   d. The level of security to be provided for the courtroom, hallways, and building, etc.
   e. Whether or not a security screening station shall be used outside the courtroom etc.

b. The Chief Inspector - Uniform Services, or designee, shall also be accountable, and have full authority and responsibility for the operational planning guidelines of a High - Risk Trial.

c. The Chief Inspector - Uniform Services (Criminal Operations), or designee, shall create, design, and implement a security operational plan for high risk trials. The Chief Inspector - Uniform Services, or designee, shall coordinate internally with the Philadelphia Sheriff's Homeland Security Unit, and externally with all other agencies involved in the High - Risk Trial (state/local police, federal agencies, the court administration, Fire Department, and EMS, etc.).
d. The Chief Inspector - Uniform Services, or designee, shall ensure that intelligence information is collected, (via courtroom, prisoners, radio, newspapers, family/audience members, other law enforcement agencies, etc.) and is disseminated to everyone involved in the security/operational plan.

e. Each plan shall be re-evaluated and updated to remain flexible and adaptable; addressing the dynamic nature and nuances involved in protecting stakeholders in High Risk Trials. The introduction of new information requires re-evaluation, open communication, and coordination to be successful.

f. The Chief Inspector – Uniform Services, or designee and the Presiding Judge/Court Administration shall select a suitable courtroom for the security of the high risk trial (i.e., a courtroom with close proximity to the detention area, elevators, stairs, crowd control, interior/exterior courtroom space, separated spectator area, best courtroom placement for the most expeditious security response, and deployment of personnel, relief units, etc.)

g. The Chief Inspector – Uniform Services shall also ensure communications between assigned personnel, departments/agencies participating in the trial security are predetermined and uniform. The Chief Inspector – Uniform Services, or designee, shall ensure all sheriffs’ deputies are equipped with two-way radios, and the plan delineates all deputies’ call signs, identifies primary and secondary radio bands, etc.

h. The Chief Inspector – Uniform Services, or designee, shall conduct a pre-plan briefing for deputies to familiarize them with the operations plan and specific procedures for a high-risk trial.

i. The Chief Inspector - Uniform Services, or designee, shall establish daily search procedures for deputies that shall be conducted prior to the opening of the courtroom/courthouse to the public. The daily search shall include but not limited to:

   a. All prisoner detention areas, the courtroom, judge’s robing room, all anterooms, visit booths, jury areas, bathrooms, elevators, vehicles, etc.

   b. When the courtroom search has concluded a deputy shall maintain on site security of the room ensuring no weapons can be hidden.

j. The Chief Inspector - Uniform Services, or designee, shall designate deputies to operate a security screening device to monitor each spectator entering the building/courthouse.

k. When a high-risk trial generates local or national news the Sheriff, or the communication/media – PIO, shall be the only deputy/employee responsible for daily communication with the news media. No one else employed in the Office of the Sheriff shall provide comment(s) to the news media without approval from the
Sheriff or designee. This would include but not limited to, high risk trials, any operations, incidents, transportation duties, uniformed services duties, supervision, warrants, incidents of witness intimidation, etc.

1. The Chief Inspector – Uniform Services, or designee, shall ensure an official debriefing meeting occurs after the high-risk operation to critique the operational strategy and to promote planning improvements in the next high-risk operation.

m. Sheriffs’ Homeland Security Unit shall be notified.

BY ORDER OF:

[Signature]

DATE

SHERIFF
XVI. PURPOSE:

A. The purpose of this Directive is to establish a policy in the unlikely event of a prisoner escapes from members of the Sheriff's Office of Philadelphia.

XVII. POLICY:

A. All deputy sheriffs employed and empowered by the Philadelphia Sheriff's Office shall conform to the following policy.

a. When a prisoner escapes from custody, either from a courtroom, courthouse, detention area, jail, vehicle, hospital, etc. the following procedures shall be implemented without delay:

   a. The deputy who had custody of the prisoner shall notify a supervisor and other working deputies via radio.
   b. The deputy who lost the prisoner shall also instruct courtroom, jail, hospital, etc. personnel (when the subject is not immediately apprehended) to "Activate the Duress Alarm and/or phone the deputy sheriff supervisor or designee", and notify the transportation or CJC desk sergeant of the escape.
   c. The deputy shall always pursue the prisoner and attempt to affect an apprehension (if uninjured).
   d. The supervisor/deputy receiving the notification shall:

      1) Broadcast the prisoner escape, over their radio for other deputies to respond; calling the courtroom and gathering all pertinent (flash info) information concerning the prisoner escape (i.e., prisoner name, police photo number (PPN), charges, location/direction, shirt color, pants color, height, weight, race, etc.).
   
      2) Relay all flash information immediately to the cell room supervisor, Uniformed Services Captain and below, and Warrant Unit deputies for support.
e. The cell room supervisor will obtain a picture and criminal history of the escaped prisoner and ensure that information is communicated to all deputies via Everbridge, email, fax, etc. The prisoner's picture shall be distributed to all Sheriffs' Office and local law enforcement personnel/police for deputy safety and to facilitate their swift identification, location, and re-arrest.

b. When a prisoner escapes from a vehicle, house, or street (and the subject is not immediately apprehended) the deputy shall broadcast the escape over sheriff radio, inform his/her immediate supervisor, and notify the local jurisdiction or police department, including all pertinent information (see II, A, D, 1-2).

a. The Uniformed Services and/or Warrant Unit Captain(s) shall be notified immediately of the escape.

b. The Uniformed Services and/or Warrant Unit Captain(s), or designee shall notify all deputies of the escape by radio (i.e. bike patrol, K-9 units, warrant unit, etc.).

c. The affected Deputy Chief or designee shall notify the Sheriff and Chief Deputy of the escape via Everbridge.

d. The first supervisor notified shall ensure procedures are enacted to seal all exits and to secure the perimeter, including but not limited to:

1) Instructing the desk supervisor to notify the local police department of the escape, flash information, and request assistance in securing the perimeter and locating the escapee.

2) When the subject is not immediately apprehended, instruct members of the Warrant Unit of the escape, and inform the Warrant Unit Supervisor of all pertinent information.

3) The Warrant Unit shall respond to the location, assumed investigative authority, pursue and attempt to apprehend the escape prisoner.

i. Warrant Unit involvement does not preclude the reassignment of uniformed services deputies to fugitive location and arrest duties.
Philadelphia Sheriff’s Office

DIRECTIVE: #15
SUBJECT: FUNERAL DETAILS
ISSUE DATE: 05-11-2020
REVISED DATE: 02-24-2021

XVIII. PURPOSE:

A. The purpose of this directive is to establish a policy on prisoner security during a Funeral Detail when performed by members of the Sheriff’s Office.

XIX. POLICY:

A. All Philadelphia Sheriff’s Office employees shall conform to the following policy:

1. All Philadelphia Sheriff’s employees shall direct all funeral petition requests to the petitioner’s attorney or the public defender (215-568-3190). Sheriff’s Office employees shall further instruct persons requesting funeral petitions to have their attorney or public defender to contact the Criminal Justice Center cell room, for risk and safety assessment.

2. The Deputy Chief-Uniform Services, or designee, shall be responsible for the administration of all prisoner funeral assignments.

B. The Deputy Chief-Uniform Services, or designee, shall review and approve all pertinent operational information regarding a funeral detail.

1. All available prisoner information shall be utilized including:

   a) Criminal history
   b) Prisoner institutional records
   c) Prison disciplinary reports
   d) Family information
   e) Gang/crime affiliation
   f) Last known address (LNA), frequented locations, locations of arrest, etc.
   g) Media: television, internet-media, newspapers, radio, etc. to determine the level of security risk
3. If the Deputy Chief-Uniforms Services or designee determines the risk to the public, deputies or the defendant is too high to allow for a funeral detail to take place, she/he shall inform the attorney or public defender and the Civil Enforcement supervisor of the Sheriff’s Office Main Filing Desk of the denial of funeral prisoner escort.

4. If the Deputy Chief-Uniform Services or designee determines the risk to the public, deputies, and defendant to be minimal, she/he may approve of the funeral detail. Once approved the Deputy Chief or designee shall notify the Civil Enforcement supervisor of the Sheriff’s Office Main Filing Desk. The Deputy Chief-Uniform Services shall direct the petitioner’s attorney or the public defender to send the petitioner to 100 S. Broad St., the Main Filing Desk with a completed funeral petition, detailing prisoner’s name, institution, church or funeral parlor and date and time of funeral.

5. The Sheriff’s Office Main Filing Desk Clerks shall accept payment for the funeral petition in the form of cashier’s check, money order or attorney’s check, in the amount of $66 for petitioners in Philadelphia County facilities and $86 for all foreign county petitioners. It shall be noted that the City of Philadelphia’s Home Charter (See: Chapter 10; section 1002) only allows funeral details from Graterford Prison. The clerk shall process and file the petition within the Sheriff’s Office electronic filing and case management system.

6. All foreign county (security) approved funeral petitions shall be submitted to the Undersheriff for legal authorization before filing at the Main Desk. It is the responsibility of Deputy Chief—Uniform Services to ensure that the Undersheriff is apprised of security approved funeral petitions.

C. Once the administrative aspects of the funeral detail have been completed, the Deputy Chief-Uniform Service ensure that the following policy is adhered to:

1. All prisoners present security risks, therefore, when accommodating an order relating to facilitating a prisoner funeral detail the Transportation Captain shall create an operation plan inclusive of all deputies and resources utilized during the funeral details.

   a) The Transportation Captain shall obtain written approval for the operations via endorsement on the plan from the Deputy Chief- Uniformed Services.

   b) The Transportation Captain shall ensure the prerequisite numbers of deputies are assigned with a supervisor to safely execute the funeral detail.

   c) The Transportation Captain shall ensure the prerequisite number of vehicles, radios, and equipment, are allocated to the plan to conduct a safe and effective funeral detail.
d) The Transportation Captain shall designate a hospital vehicle for the detail and map the closest hospital/trauma center routes as they relate to the pre-established funeral locations(s).

e) The Transportation Captain shall contact each respective police district(s) or jurisdiction(s) prior to the detail, provide them a photograph and pertinent details of the prisoner, advising them a prisoner is attending funeral services in their area.

f) The Deputy Chief – Uniformed Services via endorsement acknowledges that all information provided in the operations plan is correct and that all mandatory notifications shall be communicated pursuant to this directive.

XX. PROCEDURE:

A. The funeral detail supervisor (sergeant or above) shall send out a scout patrol for reconnaissance at least one (1) hour before the funeral. The scout patrol shall continue throughout the funeral detail and shall not end until the funeral detail has vacated the area. The scout patrol shall follow the funeral detail at a safe distance, until the prisoner has been returned the holding facility. The supervisor may cancel the detail if reconnaissance reports prove the detail a risk to the public, deputies, and the defendants.

B. The funeral detail visit shall occur at least thirty (30) minutes before the start of the funeral.

C. The funeral detail visit shall not exceed fifteen (15) minutes in duration.

D. The Funeral Writ shall accompany deputies working the funeral detail to the funeral parlor.

i. The funeral writ shall be signed and dated by the funeral director or designee indicating the prisoner was on location for the viewing.

ii. The Deputy Sheriff (sergeant or above) supervisor shall indicate the prisoner’s time in and time out of the viewing on the writ.

iii. At least two escorting deputies other than the supervisor shall witness and sign their names, badge numbers, vehicle numbers, etc., on the funeral writ.

iv. The funeral writ will be returned to the Transportation Captain and filed with the operations plan and all filed paperwork.

E. Deputies shall always be responsible for the prisoner in his/her custody. Deputies are also responsible for the safety of the public, therefore if a prisoner escapes, or attempts to escape the deputies shall pursue the escaped prisoner in the attempt to affect an arrest and follow directive #14.
F. Deputies shall utilize a marked vehicle on funeral details unless otherwise specified by the Transportation Captain. Deputies shall park their vehicles close to building entrances/exist, etc.

G. Deputies shall not permit a prisoner to fraternize and/or engage in any physical contact with friends or relatives.

H. Deputies shall notify radio of their departures and arrivals at the funeral home to their operational base.

I. Deputies shall keep a vehicle log of all locations, arrivals, departures, and inmate movement.

J. Deputies shall maintain a professional, pleasant, confident public image.

K. Deputies shall inform the Uniformed Services Captain or designee of the successful conclusion of the detail once the prisoner is returned to the jail.
DIRECTIVE: #16
SUBJECT: HOSPITAL AND TRANSPORTATION DETAIL
ISSUE DATE: 05-11-2020
REVISED DATE: 02-24-2021

I. PURPOSE:

A. The purpose of this directive is to establish a policy on prisoner security during hospital details when performed by members of the Philadelphia Sheriff’s Office.

II. POLICY:

A. All deputies in the Philadelphia Sheriff’s Office shall conform to the following policy:

1. The Sheriff, or designee, shall provide security; retain custody and maintain control over any/all prisoner(s) who require(s) hospitalization in their charge.

2. Deputy Chief-Uniform Services, or designee, shall be responsible for the effective administration of a hospital visit.

3. The Chief Inspector-Uniform Servicers or Inspector (if applicable), or designee, shall upon notification of a hospital detail, ascertain the following information:

   a. The name of the prisoner.
   b. The prisoner’s criminal charge(s).
   c. Make the determination whether to classify the prisoner as a “high” or “low” security risk, detailing the reason for such status in the incident report.
   d. Provide the name of the applicable hospital/medical facility and transportation unit numbers.
   e. Cite the location/address/telephone number of the hospital/medical facility and their security contact.
   f. Include the telephone number of the hospital/medical facilities emergency/hospital room(s) of the prisoner(s).
g. New commit(s) requiring medical treatment shall be transported. The commit and retain order shall remain with the prisoner.

h. Inquire if the emergency room can accept prisoner(s) according to security protocols.

4. The Transportation Captain, or designee, shall notify the assigned deputies of the high-risk status of the prisoner and the operational safety measures to be employed.

5. The Transportation Captain, or designee, shall visit the hospital/medical facility during the initial work shift to ensure all safety and security procedures are being followed.

6. The Transportation Captain, or designee, shall insure each deputy on the hospital detail is issued a Sheriff/Police band radio(s) and cell phone(s).

7. Sheriff’s Office Transportation Vehicle:

a. In the event a prisoner is transported by an emergency ambulance from the detention unit/accident scene, the Transportation Captain, or designee, shall notify the Deputy Chief or Chief Inspector-Uniform Services.

b. The Transportation Captain shall ensure at least two deputies secure a prisoner, one deputy in the (non-Deputy Sheriff) emergency vehicle, and one deputy in a marked Sheriff vehicle driving behind the emergency vehicle. For any unusual or special circumstances contact the Unit commander or his designee for instruction.

c. The deputy assigned to the hospital/medical facility shall search the hospital room/area at the beginning of the detail for weapons. The room shall be searched at the beginning of each succeeding shift, when relieved, and/or when necessary by the assigned deputy.

d. The deputy assigned to the hospital/medical detail shall ensure that the prisoner is never left unattended at any time.

e. The deputy assigned to the hospital detail shall ensure that the telephone calls to the prisoner or by the prisoner are not allowed.

f. The deputy assigned to the hospital/medical detail shall ensure that the prisoner is supplied with plastic utensils only for meals.

g. The deputy assigned to the hospital/medical facility shall not permit visitors to enter the prisoner’s room.

h. The deputy assigned to the hospital/medical facility detail shall accompany the prisoner when s/he is moved from one location to another within the facility for the purposes of testing, x-rays, MRIs, etc. Handcuffs or leg restraints shall be utilized, on the prisoner in custody, in a manner which will impede freedom of movement, but not precludes the examination.
1) The deputy shall not argue with the hospital staff, who wishes to perform tests on a subject in custody requiring restraints.

2) The deputy shall document that decision on an incident report as hospital case – prisoner.

8. The deputy assigned to a hospital/medical facility detail shall wear the uniform of the day including and all prescribed issued equipment.

9. The Transportation Captain Commander, or designee, will issue any other special instructions/orders concerning hospital/medical facility transportation or details, if necessary.

III. This directive supersedes all other hospital detail policies.

IV. This directive is effective immediately.

BY ORDER OF:

[Signature]

SHERIFF DATE
Philaidephia Sheriff's Office

DIRECTIVE:          #17
SUBJECT:            TRANSPORTATION OF PRISONER(S) VIA AIRCRAFT
ISSUE DATE:         05-14-2020
REVISED DATE:       02-24-2021

I. PURPOSE:

A. The purpose of this directive is to establish a policy for Philadelphia Sheriff's Office deputy sheriffs who transport prisoners and carry firearms aboard an aircraft.

II. POLICY:

A. The policy of the Philadelphia Sheriff's Office is to cooperate with the Federal Transportation Safety Administration (TSA) guidelines by adhering to the established procedures regulating law enforcement officers who carry firearms when transporting prisoners aboard commercial aircrafts.

B. The regulations governing carrying firearms while transporting prisoners aboard commercial aircrafts in the United States are found in the Code of Federal Regulations (C.F.R.) Title 49 Chapter 12 subsection 1544.119 – Carriage of accessible weapons, and subsection 1544.221 – Carriage of prisoners under control of armed law enforcement officers.

C. Deputies shall be knowledgeable concerning these regulations and shall only carry a firearm on a flight after successfully completing the prerequisite TSA training relating to law enforcement officers who carry firearms on aircrafts.

III. PROCEDURES:

A. Pre - Flight

1. The applicable deputy chief or designee, shall ensure that any deputy assigned to escort a prisoner on airline qualifies for AND has already completed the Law Enforcement Flying Armed training program described below:

118
a. Flying Armed: to qualify to fly armed, unless otherwise authorized by
TSA, federal regulation states that a law enforcement officer must meet all
the applicable requirements for a deputy sheriff:

1) Be a full-time municipal, county, state, tribal or territorial law
enforcement office who is a direct government agency employee.

2) Be sworn and commissioned to enforce criminal or immigration
statutes.

3) Be authorized by the employing agency to have the weapon in
connection with assigned duties.

4) Completed the TSA Law Enforcement Officer Flying Armed Training
Course.

5) In addition to the above requirements, an operational need to have the
weapon accessible from the time he or she would otherwise check the
weapon, until the time it would be claimed after deplaning. The need
to have the weapon accessible aboard the aircraft must be determined
by the employing agency and based on one of the following:

- Assigned to a protective duty as a principal or advance team, or
  on travel required to be prepared to engage in a protective
  function.
- On official travel with a requirement to report to another
  location armed and prepared for duty immediately upon
  landing.
- Control of a prisoner, or on a round trip ticket returning from
  escorting or traveling to pick up a prisoner.

2. Sheriff’s Office & TSA Complaint – Training Program

a. Since the Sheriff’s Office has an operational need for deputies to fly
armed, the Deputy Chief Training is the single instructor/point-of-contact
to request any training or materials,

b. This point-of-contact must request the training material to instruct the
Sheriff’s Office deputies within their agency who meet federal regulations
to fly armed by completing the fill-able form provided at the following
link: https://www.tsa.gov/travel/law-enforcement

c. The Deputy Chief - Training shall request all training materials and serve
as the instructor/point-of-contact for the Office of the Sheriff: Request
Training Materials and as required below:

1) Be a full-time law enforcement officer meeting the instructor
qualification standards of their agency.
2) Click on the below Request Training Materials icon and complete all required information.

3) Send the request from a government email.

3. As a recognized law enforcement agency who authorizes officers flying armed, the Deputy Chief-Uniformed Services shall ensure:

   a. A National Law Enforcement Telecommunications System (NLETS) message is sent to TSA at least 48 hours prior to travel. The NLETS message is sent to the TSA via PPD Radio (M Band or T Band).
   b. Each deputy assigned to the escort detail receives and travels with two (2) copies of the paper and email copies of the NLETS receipt(s) generated by that notification.
   c. The Deputy Chief-Uniformed Services, or his/her designee, shall ensure that all court orders are complete and are verified prior to making travel arrangements.

4. The Deputy Chief-Uniformed Services, or his/her designee, shall ensure that the necessary travel arrangements are booked only with an approved travel agent.

   a. The Deputy Chief is fiscally responsible for checking a minimum, three (3) online travel outlets for pricing comparison, to ensure the actual itinerary prices proposed by the travel agent are lower than prices gleaned through their internet research.
   b. Unless authorized by the Sheriff or Chief Deputy, no travel shall be booked in business class or first class.
   c. Booked seating shall be requested at check-in for deputy safety.

1) Deputies shall request to be assigned to the last row on the plane and position the prisoner next to the window.
2) One deputy shall sit in the seat next to the prisoner between the prisoner and the aisle.
3) In keeping with sound weapon retention tactics, a right-handed deputy shall sit next to the prisoner when the two are seated on the left side of the plane and a left-handed deputy shall sit next to the prisoner when the two seated on the right side of the plane, whenever possible.

5. The Deputy Chief-Uniformed Services will determine the security level necessary for the escort taking into consideration the subjects charges, profile, and history, and shall ensure that enough personnel are assigned to conduct a safe escort.

   a. The compliment of deputies escorting a prisoner(s) on a commercial aircraft shall exceed the number of prisoners being escorted by at least
one. For example, one prisoner shall be escorted by not less than two deputies or two prisoners by not less than three deputies.
b. At least one deputy shall be the same gender as the prisoner being escorted.

B. Dress and equipment

1. Deputies shall have a full complement of restraints including but not limited to:
   a. Handcuffs, black box, traveling belt and leg irons as well as any other departmentally issued restraining device deemed necessary to accomplish a safe escort.

2. Deputies shall dress in a business-like manner including pants, a jacket, and collared shirt (tie is optional).
3. Female deputies shall dress in a pants suit and jacket. Shoes should be low heeled or flat.
4. Deputies shall carry their issued service weapon and spare magazine on their person, always during the escort.
5. No deputy weapons or ammunition shall be stored or carried in carry on or checked bags.
6. Deputies shall carry their department issued credentials on their person while conducting an escort.
7. Deputies shall ensure that all required paperwork including tickets, TSA authorizations, notification to airlines letters and writs/warrants/waivers and departmentally issued credit cards, when necessary, are in their possession prior to departing for escort detail.
8. Pepper spray is expressly prohibited by federal Regulations on commercial aircraft and shall not be carried on a deputy’s person.
9. Baggage checked in may have the approved amount secured.
10. Carrying of ANY/ALL secondary weapons must receive pre-authorization from the Sheriff or Chief Deputy.

C. Preparing prisoner for transport

1. Prisoners shall be thoroughly searched prior to transport.

2. 49 C.F.R. subsection 1544.221(g) mandates that “each armed law enforcement officer escorting a prisoner and each aircraft operator must ensure that the prisoner is restrained from full use of his or her hands by an appropriate device that provides for minimum movement of the prisoners hands and must ensure that leg irons are not used”. The following supplemental restraints may be used:
   a. Black box and padlock.
b. Belly chain and leg brace.
c. Leg irons: may not be worn by a prisoner while he/she is on the plane but shall be worn by a prisoner while in transit between detention facility and airport. Leg irons shall be removed at a suitable area, such as the airport police station before escorting the prisoner through the airport concourse.
d. Supplemental restraints may be applied at any point if deemed necessary in the judgment of the transporting deputies, including the airplane, with the concurrence of the pilot.

3. Deputies shall cover the restrained prisoners' hands with a jacket or shirt so as conceal the restraints from public view. Deputies and their prisoner should attempt to remain anonymous by concealing all Sheriff related equipment whenever possible.

4. Deputies shall always maintain physical control of all prisoners in or around the airport.

D. Upon arrival at airport

1. Deputies shall arrive at least two (2) hours prior to takeoff.

2. Deputies shall check-in at the ticketing counter to advise the airline of law enforcement officers transporting a prisoner and flying armed. Deputies shall present their credentials, badges, identification cards, driver's licenses, TSA forms and Notification to Airlines of LEO Flying Armed letters.

3. Deputies shall ensure seat assignments comply with this directive.

a. Deputies shall request to be assigned to the last row on the plane and position the prisoner next to the window. One deputy shall sit in the seat next to the prisoner between the prisoner and the aisle. In keeping with sound weapon retention tactics, a right-handed deputy shall sit next to the prisoner when the two are seated on the left side of the plane and a left-handed deputy shall sit next to the prisoner when the two seated on the right side of the plane, whenever possible.

4. Deputies shall report to the TSA LEO lane at the airport and present their credentials along with the TSA NLETs receipts of notification and shall complete the required TSA in-airports forms.

5. Deputies shall then report to the TSA security screening stations and present their credentials and completed forms to the TSA Supervisor, and should not be subject to search.

E. Boarding/seating on plane
1. Deputies shall request to be the first passengers to board the aircraft and the last to debark.

2. Deputies shall ask if any other law enforcement officers are traveling on the flight and ascertain which seat numbers law enforcement personnel will occupy.

3. Deputies shall introduce themselves to the airline pilots, identify the prisoner, and determine if either is flying armed.

4. Deputies shall ensure that no prisoner shall be permitted to leave his/her seat to use the restroom or for any other reason without deputy escort. Deputies shall direct prisoners to use the restroom before boarding aircraft.

   a. If a prisoner has an urgent need to use the restroom in-flight, deputies shall coordinate fulfilling that request with the stewardess and shall not permit a prisoner the opportunity to lock him/herself in the restroom or to be unaccompanied near an exit door.

   b. A deputy shall position his/her foot in the restroom doorway to prevent it being closed while still allowing enough privacy for the inmate to attend to his/her needs.

5. Deputies shall not allow prisoners to possess any cutting or spearing implements with any meal he/she is served. Whenever possible, meals not requiring utensils shall be requested by deputies for prisoners.

6. Deputies shall not permit a prisoner to sit next to a normal or emergency exit.

7. For the comfort of their fellow passengers, deputies shall endeavor to remain anonymous during an escort. The unnecessary display of equipment or weapons is prohibited.

8. No deputy shall consume alcohol while conducting a prisoner escort by commercial airline nor shall he/she permit a prisoner to be served alcohol.

9. If another passenger, other than the prisoner, becomes unruly in flight, deputies will not take any action unless/until requested by the flight crew. The flight crew has been trained and is equipped to handle unruly passengers. Your priority is the absolute control of your prisoner.

10. In the event of skyjacking, carefully evaluate the situation and condition with your partner(s); and act when the opportune moment presents itself. Refrain from unnecessary actions that might further jeopardize the safety of the passengers or the flight.
11. Deputies shall always cooperate with TSA officials and representatives of the airline. It is the prerogative of the responsible representative of the airline to refuse transportation of the deputy and the prisoner at any time. If for any reason transportation is denied, deputies shall contact their immediate supervisor for assistance.

12. Deputies shall remain cognizant that many commercial airline pilots on the Flight Deck are armed. Pilots who complete TSA training have been deputized as federal law enforcement officers. Those pilots are issued a TSA-approved firearm, federal flight deck officer credentials, and are authorized to carry their firearm onboard an aircraft. Outside of the flight deck, their weapon(s) must be transported in locked cases.
DIRECTIVE: #18
SUBJECT: WARRANT UNIT PROCEDURES
ISSUE DATE: 05-14-2020
REVISED DATE: 02-24-2021

1. PURPOSE:

A. The purpose of this Directive is to establish a policy guiding Warrant Unit procedures performed by members of the Philadelphia Sheriff’s Office.

2. POLICY:

A. Philadelphia Sheriff’s Office members shall conform to following policy:

1. The Unit Commander shall ensure that every deputy in the Warrant Unit knows that the execution of a warrant must be done within the bounds of the reasonableness requirement of the Fourth Amendment of the United States Constitution. The reasonable requirement places a duty on every deputy serving warrants to knock and announce her/his Office, authority, and purpose and in effect be refused admittance to the dwelling before breaching entrances. **NO deputy shall serve a “No Knock Warrant” unless the subject of the warrant is narcotics and the Unit Commander has given approval.**

2. The Unit Commander has discretion to authorize deputies to serve a “No Knock Warrant,” only under the following conditions:

   a. When Warrant Unit Deputies have reasonably shown through surveillance notes that to “Knock and Announce would pose a severe threat to the lives and safety of the deputies serving the warrant.

3. The Warrant Unit Captain or his/her designee shall be responsible for complete and effective operation of Warrant Unit.

4. The Warrant Unit Captain or his/her designee shall implement procedures to ensure control over all incoming warrants.
5. The Warrant Unit Captain or her/his designee shall ensure incoming warrants are screened for completeness, prior to being recorded. She/he shall return all incomplete warrants to the issuing authority.

6. The Warrant Unit Captain or her/his designee shall all incoming warrants are immediately time stamped and verified for authenticity. She/he shall ensure that all warrants contain proper seals and judges' signatures.

7. The Warrant Unit Captain shall ensure that the following procedures are observed by all deputies processing and serving warrants.

   a. Deputies shall be professional when
   b. Deputies shall be alert for potential dangers and excise caution.
   c. The use of force to affect an arrest shall be in conformance to Directive #1-Use of Force.
   d. Deputies shall maintain updated and orderly files for their area of responsibilities.
   e. Deputies shall not provide a warrant (or information regarding a warrant) to an individual for service other than law enforcement personnel and only after approval of a Warrant Unit Captain, or designee.
   f. Distribution of warrants to other law enforcement agencies shall require the approval of the Warrant Captain or designee.
   g. Incidents involving deputies shall require a written Incident Report. The report shall be submitted by the end of the assigned work shift.
   h. No warrant service shall be made without notification and permission of Warrant Unit Captain or designee.
   i. Warrant services are not to be attempted without a partner, sufficient back up and operations plan.
   j. Deputies shall have all assigned and necessary equipment when serving warrants.

1. Equipment includes but is not limited to a ballistic vest, extra magazine, handcuffs, a flashlight, first aid kit, etc.

B. Act 22 of 2017 excluded body cameras from Pennsylvania's Wire Act coverage so long as footage and audio are captured by an approved recording device and statements are made in the presence of readily identifiable law enforcement on official duty. Deputies must remember that when in the homes of suspects, innocent people may be in the line of the body camera's focus and all caution should be taken as not to record persons who may not be fully clothed or in some other intimate situation. For this reason, deputies shall announce to dwellings' occupants that body camera are active and recording.

   BY ORDER OF:

   [Signature]

   SHERIFF    DATE


126
DIRECTIVE: #19
SUBJECT: USE OF LAW ENFORCEMENT VEHICLES
ISSUE DATE: 05-13-2020
REVISED DATE: 02-24-2021

I. PURPOSE:

A. The purpose of this Directive is to establish a policy on the use of city vehicles by members of the Philadelphia Sheriff’s Office.

II. POLICY:

A. Deputies serving in the Philadelphia Sheriff’s Office shall conform to the following policy.

1. A deputy sheriff shall only operate those vehicles for which he/she is properly and currently licensed. Deputies operating offices buses shall possess a Commercial Driver’s license, class B with a passenger endorsement and no air brake restriction. Deputies with a class B learner’s permit may operate a Sheriff’s Office bus only when accompanied by a valid class B license holder for training purposes. Permit holders may not transport prisoners until licensed.

2. Possession of a valid Commonwealth of Pennsylvania driver’s license is required of every deputy sheriff regardless of assignment. A deputy sheriff shall report any revocation, restriction, or suspension of his/her driver’s license to his/her supervisor immediately. Any deputy sheriff possession of a Commercial Driver’s License who is assigned to operate a bus shall report any restrictions to or downgrade in his/her license class, including endorsements, which will affect his/her privilege to operate a commercial vehicle to his/her supervisor before operating a bus.

3. The Deputy Chief-Uniformed Services shall assume the overall responsibilities of ensuring vehicles assigned to deputies under their command are allocated based upon need, workload, and/or special assignment.

4. The Transportation Captain shall implement procedures to ensure all Office vehicles receive regular preventive maintenance and are properly serviced.

5. The Deputy Chief-Uniformed Services, or designee, shall rotate the vehicles to obtain mileage equalization.
6. The Transportation Captain, or designee, shall prepare a report every ninety (90) to the Chief Deputy-Uniformed Services through their respective chain of command indicating they conducted a ninety (90) day inspection of all office vehicles to ensure that employees are properly caring for the vehicles and proper service is being performed to maintain the vehicles.

7. No issued equipment, especially firearms, shall be left inside of an Office of the Sheriff vehicle in a careless manner (see III-C).

III. PROCEDURE:

A. Deputy Sheriffs are responsible for the following:

1. Shall inspect his/her vehicle at the beginning of his/her tour of duty and shall report any damage, vandalism, or mechanical deficiencies to his/her vehicle or its special equipment including emergency lights and siren immediately to his/her supervisor.

2. A deputy sheriff shall search the interior of his/her vehicle when taking possession of it. At minimum, deputies shall search the floor, under the seats, gaps between seats and the walls, the area between the back rest and seat bench, vents, ash trays, and anywhere a person could hide contraband.

3. Seat and seat belts shall be examined for vandalism and seat upholstery shall be checked for tampering; interior wall and door panels shall also be inspected for signs of tampering or looseness and any deficiencies reported.

4. Inspection of all windows, security screens, padlocks, interior dividers, doors, and exterior security handles for signs of excessive wear, damages, or vandalism.

5. Check of all attached exterior equipment such as light bars and mirrors to ensure they are not loose and shall report any deficiencies to supervisors.

6. A check of the vehicle registration and insurance cards are in the vehicle.

7. The care and security of his/her assigned vehicles.

8. Locking the doors of his/her vehicles when it is unattended.

9. Ensuring that his/her assigned vehicle is always kept clean.

10. Obeying all traffic laws.

11. Wear seat belts when operating an office vehicle.

12. Safe operations of vehicles at all times.

13. Reporting any accidents or incidents involving his/her assigned office vehicle to his/her supervisor immediately, and shall complete and submit the accident report, where appropriate, and an incident report by the end of his/her tour of duty or as soon as possible.

14. In the event a Sheriff’s Office deputy must engage in a vehicle investigation (or car stop) the operator of an Office of the Sheriff motor vehicle must engage lights and sirens, prior to engaging in the stop of another vehicle (No deputy who has not received training in the enforcement of motor vehicle law, shall conduct any car stops).
a. The deputy conducting the vehicle investigation shall prepare an incident report entitled, "Car Stop (C/S)", and describe the who, what, when, where, and why, precipitating the necessity of the stop.
b. The C/S shall be submitted on the date of occurrence.
c. In the unlikely event a Bike Unit or deputy assigned to an exterior foot beat must stop a vehicle, all steps described in III-A, 14, a-b, must be followed.

B. A deputy sheriff shall not operate an office vehicle if he/she has consumed alcohol or a controlled substance or any substance which might impair their ability to safely operate that vehicle.

C. A deputy sheriff shall not leave firearms, protective ballistic vests, badges, issued identification cards or any ammunition inside of any vehicle whether on-duty or off-duty. If s/he has a private or personal weapon, ammunition and/or other issued equipment or identification stolen from any vehicle either, while exercising take home privileges in their off-duty capacity, or while on-duty as a result of carelessness, they shall be the subject of immediate disciplinary action.

BY ORDER OF:

[Signature]
SHERIFF DATE
DIRECTIVE: #20
SUBJECT: NOTIFICATION TO THE SHERIFF
ISSUE DATE: 08-01-14
REVISED DATE: 02-24-2021

I. PURPOSE:

The purpose of this policy is to establish procedures for notifying the Sheriff when an emergency or unusual incident occurs during non-business hours.

II. POLICY:

Sheriff’s Deputies and all employees of the Philadelphia Sheriff’s Office shall conform to the following notification policy. Incidences which occur during the normal course of business, during normal business hours shall continue to flow through the chain-of-command.

III. RESPONSIBILITIES

A. The Sheriff or designee shall designate appropriate personnel to be notified should an emergency or unusual incident occur. Personnel shall be designated for notification during business and non-business hours.

B. Names and telephone numbers of designated personnel shall be provided to:
   2. Philadelphia Police Department/ Police Dispatch.
   3. All Sheriff’s supervisors on duty and off duty.
   4. All courthouses Sheriff’s Security Stations.
   5. Court administrators both Municipal and Common Pleas.
   6. The Clerk of Court.
   7. President and Administrative Judges (CP/MC).
   8. The Northeast Parking Area (NEPA).
   9. Office of the Mayor
  10. President of City Council
C. Designated personnel shall assume the responsibility for immediately notifying the Sheriff, Chief Deputy Sheriff, or other appropriate personnel (in that order) should an emergency or unusual incident occur.

D. Listed below are some types of incidents which would require notification of the Sheriff.

1. Death or serious injury of an employee while on duty.
2. Discharging of an employee’s firearm against any person.
3. Any employee arrested.
4. Attempted or actual prisoner escape.
5. Any major disturbance, Injunction, demonstration affecting this office.

The above list is not intended to be inclusive. It is only intended to provide some examples of incidences when the Sheriff should be notified. Designated personnel should use their judgment for incidents not included in the above list but could be considered an unusual occurrence. However, if there is any question as to whether or not the Sheriff should receive notification......... NOTIFY!

E. Upon notification of the Sheriff, designated personnel shall be prepared to provide the Sheriff with all available information.

1. If requested, inform the Sheriff of policies, procedures, and past practices.

F. Incidences which occur during the normal course of business will continue to flow through chain-of-command.

IV. This policy supersedes all other notification policies.

V. This Directive is effective immediately.

BY ORDER OF:

[Signature]

SHERIFF DATE
Philadelphia Sheriff’s Office

DIRECTIVE:   #21
SUBJECT:   CIVIL ENFORCEMENT GLOSSARY
ISSUE DATE:   04-20-2020
REVISED DATE:   12-24-2021

I. PURPOSE:

The purpose of this directive is to familiarize Philadelphia Sheriff’s Office personnel, especially deputies with the words and terms frequently used in the delivery of legal process and the enforcement of judgments and court orders.

II. DEFINITIONS:

- **Abandonment of Levy**: The Sheriff’s return of a writ of execution to court due to non-payment of appropriate Sheriff’s fees or because the plaintiff has failed to order a sale within six (6) months after a levy on defendant’s property. (See 231 of the PA Code; section 3120)
- **Abeyance**: A temporary suspension of legal process.
- **Adult**: A person eighteen (18) years of age or older, who is not incapacitated.
- **Affidavit**: A written sworn statement.
- **Alias**: A second writ issued by the court for the same action.
- **Attorney of Record**: An attorney entered on the court record as representing a party.
- **Defendant**: The party in a lawsuit against whom the legal action is brought.
- **Exemption**: Amount of money and/or goods excluded from writ of execution.
- **Foreign Action**: Legal action received from another county or state for service in Philadelphia County.
- **Forth-with**: At once; immediately.
- **Garnishee**: A party not a defendant in a legal action but is in possession of defendant(s) property.
- **Encumbrance**: Amount of debt still due.
- **In Forma Pauperis**: A party unable to pay for the cost of litigation.
- **Injunction**: A court order to stop or limit an activity.
- **John and Jane Doe**: Fictitious names given to defendants when the real names or identification of defendant(s) are unknown.
- **Judgment**: A decision by a court or other tribunal that resolves a controversy and determines the rights and obligations of the parties involved; an order or decree requiring payment of money.
- **Judgment Cost**: The amount of money spent to bring about a Judgment. Attorney fees are not to be included.
- **Jurisdiction**: The Territory within which a governmental agency, authority or office may properly exercise it authority.
- **Levy**: A legal seizure of property to satisfy a debt.
- **Minor**: A persons under eighteen (18) years of age.
- **Nulla Bona**: No goods or effects. (Used when the sheriff is directed to levy personal property at an address, where there are no goods or effects.)
- **Personal Property**: Money, goods and other things not related to real estate.
- **Plaintiff**: A person who commences a lawsuit to obtain a remedy.
- **P.R.C.P.**: Pennsylvania Rules of Civil Procedure.
- **Property Claims**: A claim on levied property by a party, who is not the defendant in a writ execution matter.
- **Prothonotary**: Custodian of Court Records.
- **Real Property**: Property having to do with land, buildings, and structures.
- **Sheriff's Certification**: Part of writ of execution notice package that informs Plaintiff/attorney that someone other than the defendant may also claim some or all of property levied.
- **Subpoena Duces Tecum**: A court order to produce documents and structures.
- **Teste**: The date a writ was issued.
- **Venire**: “To Come”, a command to produce Jurors.
- **Waiver of Watchman**: When the plaintiff directs the Sheriff NOT to guard levied property and leave the property with the defendant.
- **Watchman**: When the Sheriff places a guard on levied property.
- **Writ of execution**: A court order directing the Sheriff to levy or garnish (attach) a defendant’s property, in order to satisfy a judgment.
- Writ of Possession: A court order directing the Sheriff to transfer possession of property to the plaintiff.

III. This directive supersedes all other Civil Enforcement Glossaries.
IV. This directive is effective immediately.

BY ORDER OF:

[Signature]

SHERIFF DATE
Philadelphia Sheriff's Office

DIRECTIVE: #22
SUBJECT: OUTSIDE EMPLOYMENT
ISSUE DATE: 05-14-2020
REVISED DATE: 02-24-2021

I. PURPOSE:
The purpose of this Directive is to establish policy on Outside Employment by members of the Philadelphia Sheriff's Office.

II. POLICY:

A. Deputy Sheriffs with the Philadelphia Sheriff's Office shall conform to the following policy:

1. Outside employment shall not conflict with the duties and responsibilities of the deputy or the interests of the office, nor interfere with or take precedence over the proper performance of any duties at any time or under any circumstances.

2. Determination of the compatibility of outside employment with the interests of the office shall be made by the Sheriff, or designee.

3. It is further noted that all members of this Office shall conform to Executive Order 2-11 which is attached and made a part of this Directive.

III. RESTRICTIONS:

A. Deputies are prohibited from working in any of the following situations:

1. When the badge, uniform or exercises of Sheriff's authority are to be used in the performance of the job, this includes obtaining any office information, records, or correspondence for a secondary employer.

2. Any employment or business which will in any way reduce their effectiveness as a member of the Sheriff's Office.
3. Deputies are not permitted to be employed in any establishment where alcoholic beverages are sold.

4. Deputies are not permitted to be employed as either a private or agency security guard.

5. Deputies are prohibited from engaging in outside employment, during periods of sick leave or injury on-duty absences.

6. Outside employment shall not be granted for any Deputy in violation of the sick leave policy.

IV. REQUIREMENTS:

A. The following requirements shall be conformed to:

1. Prior to engaging in any outside employment or business, Deputies shall submit in writing a request to their Unit Commander, for authorization using the forms submitted with Executive Order 2-11.

2. Whenever the term “POLICE” appears on the form Deputy Sheriff’s shall consider this as stating, “DEPUTY SHERIFF.”

3. Authorization shall apply to the specific location and conditions stated on the new job, new request. Any new or additional jobs shall require a new request.

4. Any Deputy with a record of excessive days off for sickness, poor work performance, or misconduct may result in a denial or revocation of authorization.

5. A Deputy engaged in outside employment shall take proper action on any offense or condition which would normally require attention.

6. Any injury, disability or illness incurred during outside employment must be reported immediately to the Sheriff, or designee.

V. AUTHORIZATION:

A. Processing of authorization for outside employment:

1. The Unit Commander shall investigate all requests for authorization for outside employment, and prior to approving/disapproving the request, ascertains if this type of employment is prohibited.

2. The Unit Commander shall forward the request to the Sheriff, or his designee, for review. Reasons for approval/disapproval shall be stated in writing by the Unit Commander.
3. The Sheriff, or designee, shall review the request. The approved/disapproved request shall be forwarded as follows:
   a. Original copy shall be returned to the requesting Deputy.
   b. Carbon copy to be filed in the Deputy’s personnel folder.
   c. A file containing all approvals/disapprovals and terminations shall be maintained.
   d. Permission for outside employment shall remain in effect until termination of employment or until cancelled by the Sheriff, or his designee.

VI. DISCIPLINARY ACTIONS:

Failure to obtain written authorization, giving false information when requesting authorization, or failure to adhere to the conditions of outside employment shall result in disciplinary action.

VII. This Directive supersedes all other Outside Employment policies.

VIII. This Directive is effective immediately.

BY ORDER OF:

[Signature]

SHERRIFF  DATE
Philadelphia Sheriff's Office

DIRECTIVE: #23
SUBJECT: SICK LEAVE
ISSUED DATE: 01-20-2021
REVISED DATE: 02-24-2021

1. PURPOSE:

A. The purpose of this directive is to establish a policy for sick leave for the Philadelphia Sheriff’s Office employees, which allows for safe deployment of personnel and timely completion of tasks.

2. POLICY:

A. Authorized sick leave with pay will be granted to an employee for absence from duty because of:

   1) Illness of non-service-connected injury.

   2) Appointments with doctors or other recognized practitioners for treatment of such illness or injury to the extent of time required to complete such appointments.

   3) Exposure to contagious disease.

B. Personnel shall be subject to visits and/or telephone calls between the hours of 7:00am and 1:00am by supervisory personnel of the Sheriff’s Office as designated by the Sheriff with the exception of the following conditions:

   1) An employee has 150 days (1200) or more of accrued sick leave will not be called or visited by any supervision for the purpose of a sick leave
check with the exception of those employees placed on the “Excessive Use of Sick Leave List”.

C. All employees, sworn and civilian, requiring a physical examination at the City of Philadelphia’s Employee Medical Services before returning to active duty from sick leave or a leave of absence must comply with the procedures as set forth in Section 15 of this directive. Compliance with these procedures is essential for completion of the physical examination and a timely return to active duty.

D. All personnel who violate the provisions of this directive shall be subject to immediate disciplinary action.

3. Sick Leave Accruals:

A. Sick leave shall be earned by each permanent full-time five-day week employee at the rate of one and two-thirds (1_2/3) working days for each calendar month of service, the total of which shall not exceed twenty (20) days in any twelve (12) months; provided, however, that employees hired or rehired on or after October 1, 1992 in classes represented by District Council 33 or District Council 47 or employees in non-represented classes shall earn sick leave at the rate of one and one-quarter (1_1/4) sick days for each calendar month of service, the total of which shall not exceed fifteen (15) days in any twelve (12) months. Provided further, that employees hired or rehired after March 30, 1993, in uniformed or investigatory classes in the Police Department or District Attorney’s Office shall earn sick leave at the rate of one and one-quarter (1_1/4) sick days for each calendar month of service, the total of which shall not exceed fifteen (15) days in any twelve (12) months, and provided further, that employees in the Deputy Sheriff series hired after July 3, 1997 shall earn sick leave at the rate of one and one-quarter (1_1/4) days for each calendar month of service, the total of which shall not exceed fifteen (15) days in any twelve (12) months.

B. Five-day work week employees in classes of positions represented by District Council 47 and in non-represented classes in the Executive and Professional category, hired after June 30, 1986, shall earn sick leave at a rate of one and one-fourth (1_1/4) days per month during their first three (3) years of service. At the end of three years of service such employees shall earn sick leave in accordance with this directive.

C. Five and one quarter (5_1/4) day work week employees hired after December 31, 1986, shall earn sick leave at a rate of one and one-fourth (1_1/4) days per month
during their first three (3) years of service. At the end of three years of service such employees shall earn sick leave in accordance with Regulation.

D. Employees in the classes in the Deputy Sheriff Pay Plan may accumulate sick leave up to a maximum of two hundred and fifty (250) working days.

4. Payment for Sick Leave:

A. An employee, upon retirement or their beneficiary upon the employee's death, will be paid for accumulated sick leave or convert to extend medical coverage as follows:

1) An employee, who has accumulated sick leave up to 2499 hours, can be sold or converted at 50% of accumulated time.

2) An employee who accumulates more than 2500 hours of sick leave can be sold or converted at 60% of accumulated time.

5. Use of Sick Leave:

A. Sworn personnel who report off sick on a working day for:

1) Two (2) hours or less - will not be charged with sick leave, providing that the employee's supervisor certifies the absence is due to illness.

2) More than two (2) hours to maximum of six (6) hours will be charged with four (4) hour's sick leave.

3) More than six (6) hours - will be charged with eight (8) hours sick leave.

6. Reporting Off Sick:

A. Non-shift employees - must notify their unit no later than one (1) hour before the scheduled start of work.

B. Shift employees - must notify the unit at least one hour before the start of the employee's shift.

C. Notification should be made to a supervisor. If a supervisor is unavailable, the employee receiving the notification will inform a supervisor as soon as possible.
All sick notifications shall include the phone number and address of the location where employees are recuperating, if it is different than what’s on file in the Sheriff’s Office and must indicate an expected date of a return to duty.

D. Employees must inform their assigned unit that they are reporting off sick, expected date of return, specific location, and phone number where confined, and name and relationship of person calling if the employee is unable to do so.

1) The Operations Desk Sergeant shall ensure this information is entered on personnel time sheets and daily sick reports to be forwarded to the Sheriff’s Office Human Resources. Another copy of the daily sick report shall be forwarded to Internal Affairs.

E. All Sheriff’s Office employees shall be required to call in only on the first day of any absence unless they will be unable to return to work on the expected date originally indicated. If unable to return to work on the original expected date, the employee must call in again giving a new expected date of return.

F. Employees shall remain at their residence or place of sick confinement until returning to duty. This will include regularly scheduled days off when preceded and followed by a day of absence for sick leave.

G. Sheriff’s Office employee may leave their place of sick confinement to visit the following:

1. Doctor’s Office
2. Pharmacy
3. Polling place
4. Place of worship
5. Retail outlet selling primarily food supplies
6. Other locations approved by the employee's Commanding Officer

H. All Sheriff’s Office employees shall notify Internal Affairs prior to departure from and when returning to their place of sick confinement. If the return is after the hours of Internal Affairs operations, then the employee shall call the Criminal Justice Center’s lobby operations desk.

1) The Internal Affairs deputy shall enter the time of the employee’s departure and return in the Sheriff’s Office electronic filing and case management system.
NOTE: The purpose of this procedure is to allow employee to leave their place of sick confinement for basic personal or injury or illness related needs. Abuse of this procedure will result in disciplinary action.

I. Abuse of this procedure in this section constitutes a violation of policy and is subject to the penalties in Section 13.

7. INJURIES INCURRED WHILE OFF DUTY:

A. Report all injuries incurred while off duty by preparing and submitting three (3) copies of an incident report within two (2) working days after the occurrence.

B. If the injured employee is hospitalized or physically unable, preparation of this form will be the responsibility of the first supervisor notified of the injury. They shall also ensure that the Unit Commander and Deputy Chief is notified of the employee's injury.

C. Distribution of off-duty injury report:

1. Two (2) Copies Safety Officer
2. Original Injured Employee

D. Whenever any employee is admitted to a hospital, their Unit Commander shall prepare a memorandum and submit it through channels to the Safety Officer.

8. MEDICAL CERTIFICATION REQUIREMENTS:

A. Sworn personnel must submit a doctor's certificate when absent for more than three (3) consecutive days. The certificate must be submitted within two (2) working days after the employee returns to work.

   1. A doctor's certificate is required of all civilian employees who are absent from work for more than two (2) consecutive scheduled working days. The certificate must be submitted within two (2) working days after the employee returns to work.

   2. All Sheriff’s Office employees placed on the Excessive Use of Sick Leave List shall be required to bring a medical certificate for all subsequent use of sick leave.
3. All Sheriff’s Office employees may produce a medical certificate for any sick day used in order to avoid the day being charged to excessive sick leave (as defined in Section 9).

B. Any Sheriff’s Office employee, who is absent for more than ten (10) work days must submit a medical certificate during each pay period unless the employee’s physician submits a written statement giving an estimated date of return to work which covers the period in question.

C. A medical certificate shall contain:
   1. Date and doctor's authorized signature
   2. Date and time the employee was treated
   3. Address and telephone number of the doctor or practitioner
   4. Date of expected return to duty

D. Medical certification is subject to investigation, which may include telephone or written communication with the doctor.

9. EXCESSIVE USE OF SICK LEAVE LIST:

A. An employee will be placed on the Excessive Use of Sick Leave List when:

1. They use a total of eight (8) sick days without a medical certificate in a calendar year.
   a. The employee will be notified by their Unit Commander after having used five (5) undocumented sick days that after three (3) additional undocumented days of sick leave during a calendar year will result in the employee being placed on the Excessive Use of Sick Leave List.
   b. The five (5) day undocumented sick warning memorandum must be given to the employee within ten (10) working days of their return to duty.
   c. The Human Resources Director shall ensure HR staff keeps and maintains accurate sick leave records and issues prompt notice to Unit Commander of employees who have used sick leave without documentation on five (5) occasions.
2. They develop a pattern of taking sick leave, which includes but shall not be limited to the following:
   a. Three or more occurrences of undocumented sick use on any specific assignment.
   b. Three or more occurrences of undocumented sick use before or after Regular Days Off.
   c. Three or more occurrences of undocumented sick use on any specific day of the week.
   d. Two or more occurrences of sick leave usage after being denied other leave.

B. An employee shall be placed on the Excessive Use of Sick Leave List for a rolling 12-month period from the time of being placed on the list, or from the time a violation resulting in disciplinary action occurs while on the list.

   1. An employee on this list must present a medical certificate for all subsequent use of sick leave.

   2. Any employee placed on the Excessive Use of Sick leave List shall not be paid for the first day of the next four (4) occasions or the next twelve (12) months, whichever is shorter. The employee will be carried "T" on time sheets for these occurrences.

C. Repeated occurrences of being placed on the Excessive Use of Sick Leave List may constitute reason for disciplinary action. Presence on this list may affect request for transfer and eligibility for promotion.

D. An employee with a sick leave balance of 800 hours or more shall be not be placed on this list without a formal inquiry with the Sheriff or their designee and a Fraternal Order of Police (FOP) representative.

E. The Fraternal Order of Police shall be notified monthly of all bargaining unit members placed on the Excessive Use of Sick Leave List. This notification will be made by the employees' Unit Commander.

10. SICK LEAVE WHILE ON VACATION:

   A. An employee, taken ill while on vacation, may request to be carried on Sick Leave and take the remainder of accrued vacation at a later date.
B. To be effective, the request must be in writing and:

1. Submitted to Unit Commander through immediate supervisor

2. The request must contain details of illness and be supported by a doctor's certificate if on sick status for four (4) or more days.

C. The Unit Commander shall review the request and if approved forward a memorandum to the HR Director as soon as possible to affect EAR change.

D. Employees in this status are subject to all Sick Leave regulations.

11. USE OF SICK LEAVE ON A SCHEDULED HOLIDAY:

A. Sworn personnel shall be carried off "sick" on any day that they are unable to work due to illness, including holidays, with the exception of their Scheduled Days Off.

12. SICK LEAVE CONTROL:

A. The ranking officer in the Internal Affairs Unit on duty may request supervisory personnel from one of the Sheriff's Office satellites conduct a sick check where a sworn employee resides or place of sick confinement to determine the validity of absence. The Internal Affairs and supervisor performing the sick check shall record the request and the results thereof on an incident report.

B. The supervisor conducting such visits will prepare a Complaint or Incident Report (75-48), containing the date and time of visit and whether or not at home. The employee will sign the bottom of the details block.

1. An employee with 150 days (1200 hours) or more of accumulated sick leave shall not be called or visited by supervisory personnel or any other personnel for the purpose of a sick leave check with the exception of those employees placed on the Excessive Use of Sick Leave List.

2. An employee with 150 days (1200 hours) or more of accumulated sick leave shall not be called or visited by supervisory personnel or any other personnel for the purpose of
a sick leave check with the exception of those employees placed on the Excessive Use of Sick Leave List.

3. Distribution of Incident Report (75-48):

<table>
<thead>
<tr>
<th>Copy</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>White Copy</td>
<td>Internal Affairs</td>
</tr>
<tr>
<td>Yellow Copy</td>
<td>Supervisor Performing Visit</td>
</tr>
<tr>
<td>Pink Copy</td>
<td>Sick Employee’s Deputy Chief</td>
</tr>
</tbody>
</table>

4. Employees who are not at their listed residence or place of sick confinement when visited by a supervisor performing a sick check and who has not notified Internal Affairs of their departure from the residence, shall report to Internal Affairs upon their return to work. Internal Affairs shall begin the disciplinary process as described in section 13 of this directive.

13. UNIT COMMANDER’S RESPONSIBILITIES:

A. The Unit Commander shall ensure that:

1. Sick leave usage for all personnel under their command is continually monitored (via EAR’S) for the purpose of identifying potential or actual excessive sick leave users.

2. An Excessive Use of Sick Leave List is established in their unit.

3. Employees are notified after having used five (5) undocumented sick days that three (3) additional undocumented days of sick leave during a calendar year will result in the employee being placed on the “Excessive Use of Sick Leave List”.

   a. The five (5) day undocumented sick warning memorandum must be given to the employee within ten (10) working days of their return to duty.

4. Any employees who violate the applicable policies as stated in this directive are placed on the “Excessive Use of Sick Leave List.

5. The employee is notified when placed on the "Excessive Use of Sick Leave List."
6. On the first day of each month a list of personnel on the "Excessive Use of Sick Leave List" is sent to the HR Director and the Fraternal Order of Police (FOP). Include the employee(s) name, rank, payroll number, district/unit, and date of placement on the list.

7. Before placing an employee with a balance of 800 hours of sick leave on the "Excessive Use of Sick Leave List," submit a memorandum to the Sheriff requesting an inquiry be held with the Fraternal Order of Police.

8. Disciplinary procedures are instituted when an employee is in violation of the applicable sections of this directive.

9. They track the sick usage of all employees who are "detailed in" to their unit and issue all five (5) day sick warning memorandums and place employee(s) on the Excessive Sick Abuse List when warranted.

14. PENALTIES:

A. An employee who violates any of the provisions of the rules and regulations as stated in this Directive shall not be paid for the days not worked and will be disciplined in accordance with the following procedures:

1st Occurrence - Written Warning
2nd Occurrence - One (1) Day Suspension
3rd Occurrence - Three (3) Day Suspension

B. The employee shall be counseled and advised by their supervisor when given the three (3) days' suspension. Prior to the meeting concerning suspension, the employee will be advised of the right to have a F.O.P. representative present.

4th Occurrence - Ten (10) Day Suspension

C. The employee will be counseled and advised by the Division head or their designee in the presence of a F.O.P. representative, if requested by the employee, when given the ten (10) days' suspension.

5th Occurrence - May be discharged
1. An occurrence is a violation of any of the provisions of the rules and regulations as set forth in this directive in a rolling 12-month period after an employee is placed on the “Excessive Use of Sick Leave” list.

2. An occurrence for a violation of any provisions of the rules and regulations as set forth in this directive for any employee that is NOT on the “Excessive Use of Sick Leave” list is based on a calendar year.

15. Request for Permission to Leave Place of Recuperation (Extending Longer the Employee’s Shift):

A. Permission:

1. Permission to leave residence or place of recuperation for a reason other than those expressed in 6, G of this directive.

2. Permission to leave shall be valid only between the hours of 8:00 a.m. and 8:00 p.m.

B. Procedure:

1. Personnel desiring permission to leave residence for reasons other than those expressed in 6; G, shall obtain a doctor’s certificate, which conveys that the employee is healthy enough to leave their residence and for the purposes of the requested permission. The certificate shall contain the following information:
   
   a. Reason for need to leave residence
   b. Probable date of return to duty

2. Prior to reporting to HR, employees shall prepare a memorandum addressed to their Unit Commander, requesting authorization to apply at HR for an application for permission to leave residence.

3. The Unit Commander shall list their recommendations on the memorandum.

4. Employees shall report with the memorandum to HR and prepare application for permission to leave residence (original and one copy) for approval/disapproval.
C. Approval or Disapproval:

1. Personnel whose applications have been approved shall receive an authorization from HR granting them permission to leave residence while off because of illness.
   
a. All authorizations shall be effective for a period of two (2) weeks, at the end of which time the employee must re-apply in accordance with the procedure established in this section of the directive.

2. Personnel whose applications have been disapproved will remain in their place of sick confinement and will abide by all provisions of this directive.

3. The employee shall notify their Unit Commander via phone as to whether their request was approved or disapproved. This information shall be entered on the employee's unit EAR reports.

16. RETURN TO DUTY:

A. Employees must submit to their immediate supervisor all certificates of treatment covering the entire period of absence.

B. When absent ten (10) or more consecutive calendar days, report to Employee Medical Services, 1901 Fairmount Avenue, for examination not later than 11 a.m. on or before the date of returning to duty.

1. Employees who are admitted to a medical facility for observation or treatment or who undergo a surgical procedure shall report to the Employee Medical Services for examination prior to returning to duty, regardless of the duration of the absence. This provision shall apply to injuries and/or conditions arising from motor vehicle accidents, as well as other causes and shall include "SAME DAY" and outpatient procedures.

2. When reporting to Employee Medical Services before returning to duty from sick leave, employees must present their Police Department identification card, and bring an original physician’s medical certificate on official letterhead containing the following information:
a. A current date
b. A signature by the treating physician only (stamps and signature from office personnel are unacceptable).
c. Dates of illness, injury, or disability
d. Diagnosis
e. Prognosis
f. Date of return to duty
g. Restrictions (if applicable)
h. Dates of hospitalization (if applicable)
i. Dates and type of surgery or delivery (if applicable)

NOTE: Medical records must accompany the physician’s certificate when an employee experiences any of the following:

a. Surgery
b. Hospitalization
c. Emergency Room Treatment
d. X-rays e. Medical treatment as the result of a motor vehicle accident

3. Employees should only report for their physicals 24 hours prior to their release date from their private physician.

4. Non-shift employees whose date of return falls on a Monday may report to Employee Medical Services on the previous Friday.

5. Shift employees whose date of return falls on the day immediately following their Scheduled Days Off may report to Employee Medical Services on the day immediately preceding their scheduled days off. However, shift employees whose date of return falls on a Monday and their squad is scheduled to work on the weekend, may not report to Employee Medical Services until Monday.

C. The Unit Operations Desk Supervisor will ensure that sick slips are forwarded to the HR and that a notation is placed in the "Remarks” section of the computerized Employee’s Attendance Report (EAR) stating that the note was forwarded.

1. The name, badge number, payroll number, and unit of the employee will be clearly indicated on each certificate.
2. A copy of this slip will be maintained in the employee's unit

17. CONVERSION OF SICK LEAVE TO VACATION LEAVE:

A. Each full-time non-uniformed employee, except a non-represented employee in the N Pay Plan, and each full-time employee in a class in the Deputy Sheriff Pay Plan may convert two (2) accumulated sick days to (1) vacation day provided the employee maintains a balance of at least eighty (80) accumulated sick days. Such conversion shall be permitted up to a maximum of ten (10) vacation days each calendar year and must be converted as full vacation days. Employees shall inform the Sheriff’s Office HR Unit, in writing, of the conversion of earned but unused sick days during the period of time from January 1 to March 31 of each year. Conversion of sick leave to vacation may only be accomplished during the above-stated period of time. The scheduling of such vacation days shall be in accordance with the provisions of City of Philadelphia’s Civil Regulation #20.

18. USE OF SICK LEAVE FOR MATERNITY RELATED ABSENCE:

A. An employee who is incapacitated as a result of pregnancy will be permitted to use sick leave as indicated below:

1) An employee who, during the term of pregnancy, is incapacitated in any way as a result of the pregnancy will be considered eligible for sick leave in the same manner as any other incapacitating illness or injury.

2) In the period prior to delivery, sick leave may be used, with the approval of the appointing authority, upon the written recommendation of the employee's doctor that the employee can no longer work.

3) Without other justification, sick leave may be used from the time of delivery forward for four calendar weeks by employees in classes other than non-represented classes and for eight calendar weeks by non-represented employees.

4) Additional sick leave may be utilized beyond the four-week post-partum period by employees in classes other than non-represented classes and beyond the eight-calendar week post-partum period by non-represented employees when:
a. Certified by the deputy's physician
b. Endorsed by the Sheriff or designee
c. Approved by the HR Director

Use of sick leave shall be limited to that accrued in accordance with the City of Philadelphia’s Civil Service Regulation #21

B. The following additional regulations will apply:

1. The deputy shall immediately notify their Unit Commander upon receiving medical confirmation of the fact that she is pregnant.

2. Upon the written approval of her attending physician a pregnant officer may continue on active duty for the first trimester (up to 12 weeks).
   a. Should the pregnant deputy desire to remain on active duty beyond 12 weeks, she may have this extended up to but not beyond 20 weeks. In order to obtain this extension, the officer must report to Employee Medical Services with a letter from her physician verifying that she can continue on active duty without risk to her pregnancy.

3. If the active duty extension is not exercised, the pregnant deputy shall be placed on restricted duty with sedentary activity. Duty beyond 20 weeks gestation shall be of a restricted nature only and will not involve any physical stress.

4. The pregnant deputy shall ensure that her attending physician keeps Employee Medical Services advised of her condition via written communication.

5. The pregnant deputy may continue to work in a restricted duty capacity unless her physician indicates in writing that her condition renders her incapable of performing such work.
6. Following delivery - return to work will not be approved until the deputy reports to Employee Medical Services with a letter from her attending physician stating that she is physically able to return to duty. Employee Medical Services will determine the type of duty status (i.e. restricted or active) to which the officer will return.

BY ORDER OF:

[Signature]

SHERIFF DATE

153
DIRECTIVE:      #24
SUBJECT:        REAL ESTATE SALES AND ENFORCEMENT ACTIONS
ISSUE DATE:     08-01-2014
REVISED DATE:   02-24-2021

21. PURPOSE:

A. The purpose of this directive is to establish a policy for the Philadelphia Sheriff’s Office-Real Estate Sales process. This directive delineates protocols for receiving, recording, processing and return of service of litigation in accordance with the Pennsylvania Rules of Civil Procedure and allows for the ethical, transparent, and efficient method of delivery service.

B. The purpose of this order, the objective of the policy is to ensure the integrity of all real estate sales and execution of civil enforcement strategies. These policies and processes are designed to promote and preserve:

3. The timely and accurate entry of Civil Action Complaints into the County Suite software system.

4. Openness, fairness, and impartial treatment of all parties of interest involved in civil matters.

5. Explicitly safeguarding the legal rights of all stakeholders by receiving, recording, and returning service of the execution and attachment, in an accurate, ethical, and efficient manner when performed by deputies of the Office of the Sheriff.

6. Neutral, transparent, and well-defined policy for scheduling and facilitation of Sheriff Sales and enforcement activities as performed by sworn members of the Office of the Philadelphia Sheriff.

22. TERMS AND PROCEDURES:
A. Civil Enforcement-Civil Actions (Service of Process) Terms:

1. Combines Assumpsit and Trespass Complaints, all other complaints should be identified as Civil Action followed by the type of action, i.e., Civil Action-Replevin.

2. **Civil Action**-in simplest terms is legal action when the Sheriff Deputy is required to serve notice upon litigants. Combines Assumpsit and Trespass complaints with all other complainants considered a Civil Action; followed by Civil Action-Replevin.

3. **Civil Action-Assumpsit**: an expressed, implied, or contracted not under seal on which an action may be brought.

4. **Trespass**: defined as unjust intrusion of property.

5. **Replevin Action**: legal action designed to recover personal property that wrongfully taken or detained.

6. **Service**: to conform with PA Rules of Civil Procedure, when a process is served by a deputy sheriff to begin litigation.

   a. **Service** is legally rendered by:

      1) By a deputy sheriff personally handing a copy of the document(s) to the defendant (See: Rule 402 (a)1)
      
      2) By a deputy sheriff handing a copy of the document(s) to a competent adult family member, who resides with the defendant, if no family member is present then by handing a copy to competent adult, in charge of residence. (See: Rule 402(a) 2i and Rule 76).
      
      3) By a deputy sheriff handing a copy of the document(s) to the clerk or manager of the apartment house, hotel, inn, boarding house, or place of lodging at which the defendant resides (See: Rule 402(a)2ii).
      
      4) By a deputy sheriff handing a copy of the document(s) to the agent or person in charge of the office or usual place of business of defendant (See: Rule 402(a)2iii).
      
      5) By a deputy sheriff handing a copy of the document to the defendant's authorization agent (See: Rule 402b).

   b. In Philadelphia County (only) original service may be done by someone other than a deputy sheriff. In all other PA counties’ deputy sheriffs are the only process servers.

   c. Some private service processors are paid via commission or receive additional funding for attempting to serve legal documents. Deputy Sheriffs are sworn
law enforcement and receive static compensation via the respective county Office of the Sheriff regardless of outcome of the service attempt. It is important to remember that an unscrupulous process servicer may fabricate the number of service attempts made, if any. **In denying a party proper service a server may deny unsuspecting victims critical due process rights of law (See: U.S. Constitution 4th and 5th Amendments) or facilitate the theft of properties in the Commonwealth.**

d. If the Sheriff and/or Office is a party to the legal matter, service shall be made by the coroner or other officer authorized by law to perform the duties of coroner (See: Rule 400c).

e. If a Sheriff is to serve a respondent in another county in PA, the Sheriff can temporarily deputize the foreign county Sheriff for the effectuation of service (See: 400d).

f. Civil Action complaints shall be serviced within the Commonwealth with 30 days of issuance by the Prothonotary (Holder of Court Records See: Rule 400)

7. **Return of Service:**

a. Returns of Service shall be complete forthwith and filed with the Prothonotary.

b. If no service is made and the writ has not been reissued or the complaint reinstated, a return of no service shall be made upon the expiration of the period allowed for service (See: Rule 405a) and shall be documented in the County Suite System. The docket sheet must demonstrate the complaint in mortgage foreclosure being filed with the court AND delineate all attempts at service.

c. Upon the expiration of the legally prescribed 30-days a new complaint must be enacted and issued.

1) The Court recognizes this as a second attempt of service and allows the mortgage company (or bank) to serve the second attempt via an alternative service. Alternative service is a lower standard of service than personal service and may be via mail, posting, or advertisement.

2) Alternate service may not circumvent legal service standards and should be able to document all such service attempts to meet judicial expectation of service.

d. A return of service shall set forth the date, time, place, manner of service, the identity of the person served, and any other facts that the court deems necessary to determine that the service is proper. (See: Rule 405(b)).
8. **Judgment:** A court order or decree mandating payment of money, stemming from the act or the failure to act of a defendant; subject to the PA Rules Civil Procedure (See: Rule 3100).

9. **Personal Property:** Personal property located in a home or business, which may become subject to a writ of execution.

10. **Writ of Execution:** A court order instructing the Sheriff to enforce a judgment against a defendant (See: Rule 3102).

11. **Writ of Execution for Garnishment (Personal Property):** A **Garnishee** is any person or legal entity deemed to be in possession of Personal Property of a defendant. Garnishment is the collection by the Sheriff of legally owned property of a defendant, but in the possession of a third party that satisfies a lawful judgment. (See: Rule 3103)

12. **Writ of Execution for Levy of Personal Property:** A **Levy** is the collection by the Sheriff of Personal Property that belongs to the defendant and located in the home or business of the defendant.

   a) Service of Writ of Execution for Attachments-To service the garnishee (the holder of defendant's property) personally, garnishee's agent, manager, officers, or person in charge of the residence or business.
   
   b) Service of Writ of Execution for Levy-To service a levy the Sheriff may at the direction of the plaintiff take manual possession of any tangible property of the defendant of which is included in levy. In this case the “Watchman” has not been waived and extra fees are to be collected for transport and storage of property (See: Rule 3109).

13. **Waiver of Watchman:** When the Watchman is waived, which is the most common method of levy the deputy sheriff shall make a complete and detailed inventory of good on a room by basis. The property is to be left in the custody of the defendant and defendant is to be advised to keep all levied goods intact and on location. Failure to comply could result in criminal prosecution (See: Title 18; section 5101).

   a) When applying/executing a levy a deputy sheriff shall inquire as to the names of all persons who may legally own the property at the location of the levy. If someone other than the defendant owns the property at the location of the levy, the deputy sheriff shall leave that person with a property claim form and complete a Sheriff’s Certification Form.

14. **Common Pleas Writ of Possession (Real Estate Eviction):** Writ to be recorded in a division docket and County Suite. Shall contain all information concerning writ, such as name of assigned deputy, date and time of service, disposition, and name of the Captain, Civil Enforcement, and contact information. Other
information should also be noted in County Suite for use at a later date as supplements.

a) **Notification:** It is the policy of the Philadelphia Sheriff’s Office to serve a copy(s) to the defendant and/or occupants. If no person(s) is available for service, then a copy of the Writ of Possession is to be posted on defendant's door along with contact information for the Sheriff’s Office Real Estate Division Captain. This is the initial 21-day notice of pending eviction.

b) **Prerequisites:** Twenty-one days (21) notice is a Philadelphia Office of the Sheriff policy and does not apply to commercial property/ orders from Orphans Court or direct orders from the court.

   i. Date and time of eviction is to be coordinated with attorney on the writ.
   ii. Another notice with the actual eviction date will be served or posted at defendants' premise.
   iii. The Philadelphia Sheriff’s Office requires a bonded moving and storage company, representative of plaintiff, and a means of entry, to be present at time of eviction.
   iv. Police assistance will only be requested if it’s absolutely necessary.
   v. Eviction is to take place with as little delay as possible.
   vi. Fixed items, heater, stove, lighting fixtures. etc. will remain within the property.
   vii. The defendant(s) and/or occupants will be allowed to take valuables, clothing and other necessities, with-in reason, with them. The address and phone number of the moving and storage company will be provided to the defendant and/or occupants.
   viii. The property will be “empty” when possession is given to plaintiff
   ix. Return of service is to include time, date, name of moving company, name of plaintiff's representative, name of deputy(s) assigned and any other pertinent facts as may prove useful at a later date.
   x. Upon completion of eviction, plaintiff or his/her representative must sign office copy of writ of possession of property.
   xi. Exceptions can and will arise because of court orders and necessity. Confer with division supervisor about doubts or special details.

15. **Municipal Court Writ of Possession (Real Estate Eviction):** The writ shall be recorded in a division docket and County Suite. It shall contain all information concerning writ, such as name of assigned deputies, date and time of service, disposition, and name of the Captain of the Civil Enforcement Unit, and contact information. Other information should also be noted in the Sheriff’s Office electronic filing and case management system for use at a later date as supplements.

   a) **Notification:** Copy(s) of a Writ of Possession is to be served upon defendant or adult person in charge of property to be taken into possession by the Sheriff. If no person is available for service, then copy(s) of this writ is to be
posted on door of said property along with contact information for the Sheriff’s Office Real Estate Division Captain.

i. Municipal Court requires a ten (10) day notice to vacate. The vacate date should be noted on return along with date and time of service, persons served, deputies name, and contact information for the Sheriff’s Office Real Estate Division Captain.

b) Prerequisites:

i. Municipal Court will issue an alias writ of possession after the required ten (10) days have expired. Upon filing in the Sheriff’s Office, a time and date for eviction will be scheduled.

ii. The plaintiff or his representative must be present at time of eviction and provide the means of entry.

iii. Police assistance will only be requested if it’s absolutely necessary.

iv. Eviction is to take place with as little delay as possible.

v. Defendant(s) and/or occupants will be allowed to take valuable clothing, and other necessities, within reason, with them. The address and phone number of the moving and storage company will be provided to the defendant(s) and/or occupants, if moving company is used.

vi. Municipal Court evictions are most often done by the "Lock-Out" method. This is when the defendant(s) and/or occupants are moved from the property, but his goods are stored and locked in said property. Possession is then given to the plaintiff.

vii. Advise plaintiff of his newly acquired responsibility for the goods left in the property. Request plaintiff or his representative to sign writ in acknowledgement.

viii. Sheriff’s return of service shall include date, time, moving company if used, deputies’ names, and all other pertinent information that may be used at a later date.

16. Common Please Writ of Possession (Personal Property): Writ to be recorded in a division docket and County Suite. Shall contain all information concerning writ, such as name of assigned deputies, date and time of service, disposition, and name of the Captain, Civil Enforcement, and contact information. Other information should also be noted in County Suite for use at a later date as supplements.

a) Notification: The vacate date should be noted on return along with date and time of service as coordinated with attorney on the writ.

b) Prerequisites:

i. Representative of plaintiff must be present at time possession is given. If a Sheriff Deputy is to break and enter, then a locksmith will be provided by
the plaintiff. Locksmith must be able to obtain access to property without causing damage to the locks or door.

ii. Writ will specify item(s) the sheriff is to take into his possession. No other item(s) may be taken.

iii. All items without serial numbers are to be identified by the plaintiff or his representative. This is to be noted in sheriff’s return of service.

iv. Possession is to be given to plaintiff or his representative unless otherwise ordered by the court.

v. Writ is only to be served at time of possession. No advanced notice is to be given.

vi. Sheriff’s return of service shall include date, time, name of person served, name of plaintiff representative, name of assigned deputies, and any other pertinent information that may be useful at a later date.

17. Writ of Seizure: Writ to be recorded in a division docket and County Suite.

Shall contain all information concerning writ, such as name of assigned deputies, date and time of service, disposition, and name of the Captain, Civil Enforcement, and contact information. Other information should also be noted in County Suite for use at a later date as supplements.

a. Writ of Seizure and copy of complaint shall be served forthwith, the court has already set a hearing date to take place within 72 hours. Alternately, writ may be served, and goods left with defendant for 72 hours. If plaintiff so directs, the goods can be directly turned over to plaintiff.

b. Upon service to the defendant or person in charge of goods to be seized, the deputy sheriff is to take possession of said property. Seized goods are to be stored in the jurisdiction of the Philadelphia Sheriff.

c. When person in possession of said property, who is not a party to the action, is served with the writ of seizure, the deputy sheriff shall notify him that he has been added as a defendant and is required to defend the action.

d. The sheriff’s return of service shall include the date and time of service, deputy sheriff’s name, name of person served, name of plaintiffs’ representative and any other facts that may be used at a later date.

e. See Rule 1075, P.R.C.P.

23. POLICY, DUTIES, AND RESPONSIBILITIES

A. Civil Process Administrative Supervisor (Main Desk)

1. Reports to the Civil Enforcement Deputy Sergeant and is responsible for the supervision, instruction, and training of all Civil Process Clerks.
2. Ensures that the clerks of the Civil Process Unit accurately and forthwith record all documents as they are received by the Philadelphia Sheriff’s Office.

3. Shall log the exact date and time that all documents are received by the Philadelphia Sheriff’s Office (See: Rule 3105) Note: This necessary because all legal documents are time sensitive and any action which hinders the forthwith delivery of legal process could be punishable by crime law. (See: Title 18; section 5101-Obstruction of the administration of law or other governmental function).

4. Civil Process Clerks
   a. Reports to the Civil Process Administration Supervisor.
   b. Responsible for receiving, recording, and processing of all mail and legal documents (non-Real Estate matters).
   c. Shall accurately and timely process legal documents. Shall expressly examine all legal documents to ensure they are unexpired, authentic, and submitted to the proper jurisdiction.
   d. Shall assist the Deputy Sheriff with case management.

5. The Civil Enforcement Deputy Sheriff Captain:
   a. Responsible for controlling and directing all activities in the Civil Enforcement and Civil Process Units.
   b. Ensures that all supervisors under her/his Command adhere to PA Rules Civil Procedure and policies and procedures directing actions within the Philadelphia Sheriff’s Office.
   c. Shall ensure the exact and accurate date and time of all legal and/or property related correspondence is logged by designated subordinates noting exact dates and times, and without delay.
   d. Records Civil Action Complaints and ensures the prompt entry of deputy sheriff names in the County Suite System on the date received.
   e. Compares complaints with the Office of the Sheriff return of service, making note via of entry into the County Suite system of the expiration date.
   f. Ensures that deputy sheriffs enter case dispositions and service attempts into the County Suite System and submit returns after attempts of service, or non-service is out of date or “not found.”.

1) “Not-Found” entries shall not be filed with the Prothonotary until the expiration date of the complaint. Action may be transferred to an alternate location.

2) The Civil Enforcement Captain (or designee) shall:
   i. Record all “Not-Found” location-based information in the County Suite System and on the Sheriff’s Return of Service.
   ii. Prioritize service attempts so all pending service duties occur within the 30-day period.
iii. Ensures postings and business services are completed on the first available duty date of the assigned deputy.

iv. Notify attorney/plaintiff of any difficulty with service after nine (9) working days.

g. The Real Estate Captain (or designee) responds to telephone calls or messages by the next business workday.

h. Ensures that employees’ reporting lost, stolen, or damaged documents, whether intentionally or accidentally submit a memorandum as rapidly as the situation permits on the date of the incident. The Real Estate Captain shall attach the deputy’s report to a separate memorandum (Commander’s Memorandum) describing the circumstances and how they might have been prevented to the Chief Deputy and the Undersheriff before reporting off-duty on the workday following the date of occurrence.

6. Deputy Sheriff

   a. Provide legal service of a Writ of Execution (Garnishee) upon any person or entity deemed to have possession of property of a defendant, e.g., an Agent, Manager, Officers, person in charge of a business, or residence.

   b. May provide legal service of a Writ of Execution (Levy of Personal Property) and take manual possession or custody of tangible property of the defendant which a plaintiff has made a levy. In this case Watchman is not waived and extra fees are to be collected.

   1) When Watchman is waived, the deputy sheriff is to make a complete and detailed inventory as possible of defendant's tangible goods. The Levied goods/items are to be left in the custody of the defendant and the defendant is to be advised to keep the levied goods intact pending further action.

   2) When making a levy the deputy must inquire as to any other person who may own property at that location. If someone may own property, the deputy will leave a property claim form for them. The Sheriff’s Certification form must then be filled out to reflect that person’s name and the form will be returned to the plaintiff/attorney along with a copy of levy sheet.

   3) Upon levy or attachment, the deputy shall mail attached envelopes containing copy of write, exemption claim form and list of protected exemptions. The deputy shall make note in his return of the date mailings and the County Suite system.

   4) Return of service shall include the date, time, mailings, and any other facts to determine if proper service has been made.
5) Request for levies without inventory when no person in charge is available will be refused. (Door-step levy)

6) Original execution levy and/or attachment with return is to be submitted to the Civil Enforcement Captain, or his designee, promptly.

7) If personal property to be levied is a vehicle, then said vehicle is to be impounded, and stored by the Sheriff. The Civil Enforcement Captain shall require a certification by any towing/storage company utilized, that adequate insurance for any towed/stored vehicle exists and is and shall be at the direction of the Sheriff, or designee. All towing and storage fees paid in advance by Plaintiff or Attorney of Record.

8) See 3100 series P.R.C.P. for other types of executions and attachments.

9) Attorney on writ is to be notified of any difficulty with service after thirty (30) working days. If writ is to be "Not-Found" attorney is to be notified within nine (9) days. All contact shall be entered and updated in the County Suite System

c. Serves as the primary public relations representative of the Philadelphia Office of the Sheriff, oftentimes in emotional, contentious real estate transactions. As such, all members of the Office of the Sheriff shall remain courteous, composed, and exercise professional at all times.

d. Is personally responsible for maintaining knowledge of PA Civil Rules of Procedure and all Office of the Sheriff Directives, policy, and procedures.

e. Serves as a public resource and furnishes information and assistance to anyone properly requesting it, if not in consistent with Philadelphia Sheriff's Office policy and procedures and not in violation of applicable statutory laws.

f. Shall not provide legal advice, only procedural advice.

g. Prepares daily reports to be submitted to the Chain of Command and notifies direct supervisors within their chain of command of any unusual conditions of signification incidents.

h. Are responsible for protecting, maintaining, and safeguarding all documents, writs, subpoenas, warrants, and certificates in their possession or under their control.

i. Assume responsibility for reporting lost, stolen, or damaged documents, whether intentionally or accidently as rapidly as the situation permits. A report must be submitted to the Unit Captain or Deputy Chief.
24. **Real Estate Deputy In-Charge (Deputy Chief, Real Estate Division)**

A. The Real Estate Deputy-In-Charge is a Deputy Chief appointed by the Sheriff who reports directly to the Undersheriff. The Real Estate Deputy-In-Charge (Deputy Chief) **WILL:**

1. Empower employees, direct, and control the overall activities of the Office of the Sheriff, Real Estate Unit.

2. Be responsible for the integrity and control of all Real Estate Sales conducted by the Sheriff's Office and related services.

3. Ensure all required duties are performed by subordinates, in particular the accurate and timely entry of data into internal systems.

4. Obtain legal guidance from the Undersheriff regarding any legal matters affecting the Office of the Sheriff.

5. Directs and trains subordinates in the proper performance of their duties.

6. Inform and advise the Sheriff via monthly memorandum through the Executive chain of command (Undersheriff, Chief of Staff, Chief Deputy, and Sheriff) of any the activities of his/her unit(s), herein the *Monthly Activity Report*. The *monthly activity report shall*:

   a. Be submitted to the Executive Staff (See 4, A6) **no later than the 3rd of each calendar month.**

   b. Contain accurate statistics detailing:

      1) All Sheriff Sale activities.
      2) Number of properties listed for sale.
      3) Number of properties stayed and a description why the court process halted.
      4) All H.A.R.T. Unit activities.
      5) All Enforcement Unit activities.
      6) The number of properties improperly listed as provided to the Office of the Sheriff by the City of Philadelphia.
      7) The list of properties by actual address, police district, and by city council district.
8) The distribution of properties by buyer name(s), physical addresses (no P.O. Boxes) and direct telephone numbers:

   i. **Distribution of properties by Sole Proprietorship, LLC, or INC., shall include an appendix with a corresponding list of other corporate names, DBAs, or AKAs, with the names and titles of all board members, shareholders, etc.**

   c. Include Legal Updates to applicable PA Statutory Law impacting Sheriff Sales, Mortgage Foreclosure Sales, Tax Lien sales, Civil Enforcement Activities, etc.

   d. Contain a quarterly (every 3-months) audit of the criminal histories of all Real Estate Division employees (sworn and civilian).

   e. Include under separate cover all confidential real estate related investigations.

   f. Conduct a monthly audit to ensure the accurate and timely response to telephone or digital inquiries. Audit shall encompass 10% of total inquires and will be submitted to the Undersheriff by the 3rd day of each month.

   g. Ensures that all legally mandatory duties associated with every sheriff sale of all personal property is completed (V, D. 1-16).

25. **POLICY-MORTGAGE FORECLOSURES**

   A. Title 231 is the statute governing the Pennsylvania Rule of Civil Procedure.

   B. Sheriff’s Sales (Mortgage Sales) are covered under the 3,000’s series of Rules.

   C. Every property sold at Sheriff’s Sale has a judgment entered against its owner (See: Rule 3001).

   D. A judgment shall be enforced by writ of execution, which has a legal life span of 90 days. The Prothonotary (The Holder of Court Recorder) issues the writ of execution to the plaintiff, who then files it with the Sheriff. The Real Estate Deputy-In-Charge shall ensure that all filing of writs of execution are filed in a timely manner, in order to prevent the expiration of the writ before a Sheriff’s Sale is conducted. (See: 3103)
E. The Real Estate Deputy-In-Charge shall ensure that Real Estate Unit staff, upon receipt of writ of execution, note the date and time it is received via timestamp and that all information is logged in the County Suite system. (See: Rule 3105).

26. SHERIFF SALE OF PERSONAL PROPERTY

A. If a Sheriff's Levy is not completed and the plaintiff obtains a stay and enters order, then that order shall be served or posted at the defendant's premise. An Office of the Sheriff contact (the Captain, Real Estate Division) contact name, and telephone number, along with the name and badge number of the deputy completing service. If the defendant complies, the deputy will then schedule a levy on the goods. If not, it is the responsibility of the plaintiff/attorney to hire a lock smith to gain entry without damaging the property so deputies can secure the premise after levy.

B. Upon completion of a Sheriff’s Levy, and if there no stay exists, are quest from a plaintiff in the action will be accepted and the property will be added to an upcoming Sheriff’s Sale.

C. Sheriff’s Sale Notifications

1. Notice of the Sheriff’s Sale shall be posted at the place of sale six (6) days before the sales date.

2. Copies of the sale notice shall be mailed to the plaintiff and/or plaintiff's attorney, and to the defendant, and logged into County Suite.

3. There may be only one (1) postponement to a new date, not to exceed thirty (30) days. Date of postponement and the new date must be called at time and place of original sale and documented in County Suite. All information concerning the Sheriff’s Sale will be recorded in the County Suite.

4. Debtor's Exemption (See P.R.C.P. 3123, 3123.1)

D. Date of Sale-Mandatory Duties

1. The Sheriff Sale of a property provides the Office of the Sheriff the right to legally break and enter pursuant to Rule 3127, PRCP.

2. The Undersheriff and the Deputy Chief, Real Estate Division will ensure:

   a. All notice of sales is posted and provided at least six (6) days prior to any sale.
   b. Sales begin on schedule (if possible).
c. Sale bill is cried out loud outside of premises. State that defendant(s) interest only is to be sold.
d. If defendant(s) have exemptions, said exemptions are to be set aside in goods or cash. Make note of debt plus costs.
e. Bidding begins with bulk bids, then piecemeal bids. The Undersheriff, through the Deputy Chief, Real Estate Division shall accept whichever is highest bid.
f. Recording of names and addresses of all bidders and shall insure the record includes Sole Proprietorships, LLCs, or INCs. Names, for the purpose of the Office of the Philadelphia Sheriff shall include a corresponding list of any other corporate names, DBAs, or AKAs, with the names, titles, and telephone numbers, of all board members, shareholders, etc.

3. Record all items sold, serial numbers if possible.

4. Record all other pertinent information that may be useful at later date.

5. Do not sell permanent fixtures, such as built in items, lighting, wall paneling etc.

6. Do not sell over the debt plus cost and interest, except when an item cannot be separated, such as a vehicle, forklift, jewels etc.

7. Sell on oldest writ when sundry writs are involved.

8. Cash or check from the attorney on writ only.

9. Complete receipt, white copy to buyer, pink copy to office cashier, and yellow copy is retained by a deputy in a receipt book. Record court term and number as well as Sheriff's number on receipt.

10. A sworn deputy deposits all monies with office cashier (immediately obtain copy of receipt), and remits all papers and information to the Captain, Real Estate Division.

11. That an employee brief/debrief of all Office of the Sheriff staff occurs before/after each sale. If liquor or pharmaceutical materials are involved, the appropriate agency must be notified before the sale take place.

BY ORDER OF:

[Signature]
SHERIFF DATE

167
DIRECTIVE: #25
SUBJECT: ENFORCEMENT OF WARRANTS & SUBPOENAS
ISSUE DATE: 05-12-1988
REVISED DATE: 05-13-2020

I. PURPOSE:

A. The purpose of this directive is to establish a policy of receiving, recording, servicing and return of service of warrants and subpoenas when performed by deputies of the Philadelphia Office of the Sheriff.

II. POLICY:

A. Warrants.

1. Warrants shall be timestamped and recorded immediately in the division docket; to include the date received, the assigned deputy's name, and disposition.

2. The Warrant Unit-Captain/Commander shall engage in a monthly review of each warrant received by the Office of the Sheriff and in the custody of their deputies.

3. The Warrant Unit-Captain/Commander will prepare a report to the Chief Deputy indicating the review of ALL served/unserved warrants (after thirty [30] days), due on the 3rd day of each month, indicating their personal review of the same information with the assigned deputy. The purpose of this review is to ascertain if proper due diligence in the service of each warrant has been employed.

III. PROCEDURE:

A. Warrant Service.

1. The Captain/Commander of the Warrant Unit will ensure deputy sheriffs do not attempt to serve a warrant alone. If the deputy charged with serving a warrant has a partner who is unavailable, the Warrant Unit Supervisor will assign another deputy to assist.

2. All sources of information are to be investigated in order to affect a quick service and arrest.
3. Minimum investigative procedures to be used are:
   a. The investigation of information contained on the warrant
   b. The world wide web, phone book, Facebook, Instagram, etc.
   c. Water Department, business privilege license, voter registration, and other public records.
   d. NCIC, PCIC, JNET, APOC, etc.
   e. Police photo and records.
   f. Employers and neighbors.
   g. Post-office.
   h. Criminal Listing, etc.

4. Whenever the party named on the warrant is arrested, they shall be transported to the place of warrant origin, police district, sheriff cell-room, or wherever indicated on warrant. This procedure is dependent on the type of warrant issued and shall be discussed with and approved by a Captain or above.

5. When warrant is "Not-Found" investigation steps are to be listed on return.

6. All warrant services are to be completed promptly and recorded in division docket.

B. Subpoenas (Witness).

1. Subpoenas are to be recorded in division docket; receiving date, assigned deputy's name and disposition are to be noted.

2. Service of Subpoenas
   a. Subpoenas are to be personal served and read to the person served, when possible - otherwise, it is to be served as a Summons.
   b. Exception: Family Court accepts service; adult family member or adult in charge of subpoenaed person's residence

3. Return of service to be submitted three (3) working days before court date, unless otherwise instructed by the court.

4. Subpoenas for records, books and papers are serviced in the same manner as witness subpoenas except that the person served is the custodian of the records, books, and papers.

BY ORDER OF:

[Signature]

SHERIFF DATE

169
DIRECTIVE: #26
SUBJECT: INJUNCTIONS
ISSUE DATE: 05-14-2020
REVISED DATE: 02-24-2021

I. PURPOSE:

A. The purpose of this directive is to establish a policy of service, enforcement, and process for engagement with violator(s) of an injunction.

II. POLICY:

A. Definition of injunction: a judicial order that restrains a person from beginning or continuing an action threatening or invading the legal right of another, or that compels a person to carry out a certain act.

1. This type of action is applied when the defendant party must stop its course of action to prevent possible injustice or irreparable harm to the plaintiff.

2. Enforcement can vary from a basic service to a large-scale operation.

3. A deputy shall be guided by the contents of the order and the instructions of her/his immediate supervisor before acting on an injunction.

B. Service:

1. When service is requested without enforcement, then service on defendant(s) shall conform to service of Civil Action. Other services may be requested, for example, reading and/or serving injunctions on/to persons involved in demonstrations and/or actively picketing.
2. The “Return/Affidavit of Service shall include the name of the persons served, the name of the deputies assigned, and all other pertinent information that may be used at a later date.

3. The supervisor shall ensure that all service and/or attempt of service shall be documented via Incident Report and enter in the Philadelphia Sheriff's Office electronic processing and case management system.

4. When enforcement is necessary, a supervisor shall survey the area of enforcement prior to conducting a service operation to determine the size of personnel and equipment needed to enforce the injunction safely and efficiently.

III. PROCEDURE:

A. Deployment to injunction sites:

1. Before authorizing a deputy to deploy, a supervisor shall conduct an operations plan briefing facilitated by the supervisor identified in section II; B,4. Each deputy shall receive copies of the operations plan, the injunction particulars, the restrictions applied to defendant(s), the criminal history of persons identified as defendant, a site description, history of legal actions at the location or by the group, and any other particulars pertaining to the safe enforcement of the injunction.

2. When significant or repeated violations of an injunction occur, the deputy sheriff supervisor shall ensure that a deputy sheriff reads the order to the violator(s) and informs the violator(s) that if they don’t adhere to the terms of the order after the reading of the injunction, they shall be arrested by the deputies on site. It shall be observed by all supervisors that this procedure shall not be enacted for light and transient violations.

3. When a deputy sheriff is confronted by a violator(s) after he has read the injunction and non-compliance is indicated by either the violators’ actions statements, the deputy shall confer with a supervisor before making an arrest. Only under exigent circumstances shall an arrest be made without conferring with a supervisor

NOTE: Pennsylvania Statutes Title 42 Pa. C.S.A. Judiciary and Judicial Procedure § 5108. Imprisonment for debt:
a. **Constitutional Restriction:** The person of a debtor, where there is not strong presumption of fraud, shall not be continued in prison after delivering up his estate for the benefit of his creditors in such manner as shall be provided or prescribed by law.

b. **Statutory Restriction:** Except in an action for fines and penalties, or as punishment for contempt, or to prevent departure from the Commonwealth, a defendant may not be arrested in any civil matter.

B. **Arrests for injunction violations:**

1. When arrests are made, the violator(s) are to be transported to the Sheriff’s cell-room to await a hearing from the issuing authority.

2. The deputy sheriff is to accompany the violators to the hearing so that she/he may testify to the facts of the arrest.

3. The violator(s) are to be identified and their names and addresses noted. The incident report and Sheriff’s Return/Affidavit of Service to include the time and date of the arrest, the name of the arresting deputy and any other pertinent information as determined by the supervisor.

C. **Injunction Actions with support from other City agencies:**

1. The Philadelphia Sheriff’s Office policies and/or procedures shall be followed at all times unless deviation has been ordered and authorized by Sheriff.

2. The deputy sheriff, who is present at or is called to an incident or situation, is always expected to represent the Philadelphia Sheriff’s Office well, by treating everyone we serve with dignity and respect. She/he shall make enforcement decisions based upon the Sheriff’s Office directives, policies, procedures, and instruction from his/her supervisor. The deputy sheriff and immediate supervisors are ultimately responsible for their decisions and actions.

D. **Routine Enforcement:**

1. The defendants, pickers or demonstrators are to be monitored and their numbers noted.
2. The deputy sheriff's profile (low or high) at any scene shall be determined by the supervisor in charge.

3. The Sheriff's Office is a distinguished participant of the injunction action and is cautioned not to present itself as a partial entity; and shall expressly avoid any appearance favoring either the plaintiff, or defendant.

4. When enforcement of the injunction is difficult or impossible because of sudden mass picketing or lack of available deputies, the supervisor in charge will contact their immediate supervisor and the Captain of the Civil Enforcement and/or Warrant Units. Once contacted each unit shall detail additional deputies to provide the additional humane resources to facilitate continued enforcement.

5. Information, verified or non-verified, received by a deputy sheriff concerning future activities of defendants, picketers or demonstrators is to be reported to the supervisor in charge via Incident Report.

BY ORDER OF:

[Signature]
SHERIFF
DATE

173
DIRECTIVE: #27
SUBJECT: ENFORCEMENT OF STAY ORDERS
ISSUED DATE: 05-13-2020
REVISED DATE: 02-24-2021

A. PURPOSE:

A. The purpose of this directive is to establish a policy that guides members of the Sheriff’s Office on receiving, recording, and processing the following stay orders, bankruptcies, petitions and appeals when received by the Sheriff’s Office.

B. POLICY:

A. Bankruptcy:

1. When received by the Philadelphia Sheriff’s Office, bankruptcies are immediately time stamped without delay. All legal action(s) shall cease, and all details, numbers and other particulars shall be recorded in both the Philadelphia Sheriff’s Office electronic filing and case management system and on the writ.

   a. If there are any questions as to the validity or authenticity of the document, any action(s) shall be postponed, and the Undersheriff shall be notified by the highest-ranking supervisor.

   b. In instances involving writs where a 180 Day Rule Bar Order is issued, the employee receiving the notice of the Bar Order shall confer with the Undersheriff and the attorney of record.

B. Orders and Stays:
1. When orders and stays are received by Sheriff’s Office employees shall immediately time stamp the document and enter the information into the Sheriff’s Office electronic filing and case management system. All extraneous details, case identification numbers and other information shall be recorded into the system.

C. Petitions and Appeals:

1. When petitions and appeals are received by any employee of the Sheriff’s Office, the documents shall be immediately time stamped without delay and entered in the Sheriff’s Office electronic filing and case management system. Legal action shall only be halted via court order. All extraneous details, case identification numbers and other information shall be recorded into the system.

BY ORDER OF:

[Signature]

SHERIFF DATE
1. **PURPOSE:**

   A. The purpose of this directive is to establish a policy and provide information relevant to the processing and service of legal documents by Sheriff’s Office personnel.

2. **POLICY:**

   A. Time Computation:

      1) The “**LIFE**” of a legal document shall be computed as to exclude the first day and to include the last of such period.

      2) Whenever the last day of any such period shall fall on a Saturday, Sunday or any day made a legal Holiday by the laws of this Commonwealth or the United States of America, such days shall be omitted from the time computation. The last day of the period, in such cases of time computation shall roll over until the next weekday.

   B. Expiration of most common legal process:

      1) Civil Action---------Expires in--------Thirty (30) days.
      2) Execution----------Expires in--------Ninety (90) days.
      3) Possession----------Expires in--------Ninety (90) days.
      4) Attachment---------Expires in--------Ninety (90) days, but execution matters for attachment (a.k.a. garnishment) are forthwith.
      5) Revival of Judgment-Expires in--------Thirty (30) days.
6) Notice of Sale (Personal Property)—Posted six (6) days prior to sale.
7) Notice of Sale (Mortgage Foreclosure)—Posted thirty (30) days prior to sale.
8) Notice of All Tax Sales---------------------Posted twenty (20) days prior to sale.
9) See yearly updated version of the Pennsylvania Rules Civil Procedure for all other process.

BY ORDER OF:

[Signature]

SHERIFF

DATE
I. PURPOSE:

A. The purpose of this directive is to establish a policy for the proper management of a crime scene when a deputy secures the initial scene or makes a recovery of crime scene evidence.

B. This directive shall also serve as a means to train and coordinate the effort of the Philadelphia Sheriff's Office with the Philadelphia Police Department (Patrol, Crime Scene Unit and Detectives) staff. This function of this directive is to ensure that all deputy sheriffs follow uniform crime scene procedures and:

1) Recognize and identify a crime scene and locate evidence therein.

2) Collect the evidence discovered (only in exigent circumstances).

3) Preserve and protect the evidence discovered.

4) Identify and interview witnesses (in IAD or Criminal Investigative Cases conduct by the Sheriff’s Office).

5) Identify suspects and link suspect to the crime scene, the evidence, and the crime for investigators.

6) Enable items collected at the crime scene to remain in-tact to be utilized as evidence towards a successful conclusion of a criminal case.
7) Overall scene security/integrity (until Philadelphia Police Department assume primary control) of the crime scene.

C. The protection and processing of the crime scene is the first order of business in law enforcement and is clearly of the utmost importance. This can only be successful when each member of the Sheriff’s Office exercises sound judgment to ensure the preservation and control of such scenes.

D. The crime scene is defined as “the area within the immediate vicinity, in which evidence is located or might be found.

II. POLICY:

A. It is the responsibility of all Sheriff’s Office personnel, regardless of rank or assignment, to protect the crime scene.

B. The Uniform Services (Criminal) Division shall have primary responsibility and authority for the protection and security of all crime scenes until the arrival of a PPD officer or detective (if needed).

C. The Philadelphia Police Department Detective Division of the district in which the crime occurred shall have the primary responsibility and authority for the investigation and examination of all crime scenes at which they are needed. The deputy sheriff supervisor shall assess the nature and seriousness of the crime. Shall notify the applicable deputy chief (and Executive Command Staff) via Everbridge and shall determine the need of a PPD Detective. The Uniform Services shall serve as liaison to Philadelphia Police Department Communications Center to fulfill the above requirement and shall notify PPD Detectives in the event of a major crime (i.e. murder, kidnapping, robberies, aggravated assaults, etc.).

D. Only the assigned PPD Detective, Sheriff’s Office IAD personnel assigned to the case and PPD Crime Scene Unit shall search a crime scene for evidence and/or contraband. If additional uniformed personnel are required, they shall be called to the crime scene by and shall fall in under the command of the highest Sheriff’s Office supervisor on location.

E. Only those persons immediately and directly connected to the investigation of the incident for which the crime scene was established shall be granted access. The assigned PPD Detective or PPD Investigative Unit Supervisor shall approve
any/all access to the crime scene and the first Sheriff's Office supervisor on the scene shall direct deputies to establish a staging area outside of the primary scene for responding officials and media.

III. PROCEDURES:

A. The first responding deputy shall prevent any possible disturbances to the crime scene, protecting it until all evidence has been collected or in major crimes, until the arrival of PPD-Crime Scene Unit and/or PPD Detective personnel. Disturbances includes:

1) Curious people, including well-meaning citizens trying to assist, or uninvolved police officers and any other officials. Prevent anyone from entering the crime scene expect Sheriff’s Office and PPD supervisors to safeguard the scene.

   a. Exceptions shall also include Sheriff’s Office and PPD supervisors and/or Philadelphia Fire Department transporting the injured or responding to conditions under their authority by law.

   b. City of Philadelphia’s Medical Examiner’s Office personnel shall be permitted to transport and investigate matters under their authority by law.

   NOTE: All of the above indicated agencies shall display all proper identification on the outermost garment or be in the identified uniforms.

2) The use of privately owned cell phone, iPads, etc., with camera/video recorders, and any other electronic device to record crime scenes, potential evidence, suspects, offenders or victim while on duty shall only be used in “Exigent Circumstances” when law enforcement equipment is unavailable and there is no other means to record the item or event.

   a. The use of non-Sheriff’s Office equipment in exigent circumstances shall be reported to Sheriff/Police investigative staff and documented on an incident report.

3) Crime scene deputies shall prevent anyone from entering the crime scene except for the following:
a. Deputies or police officers necessary to safeguard the scene.
b. EMS/Paramedics or deputies/police officers transporting the injured.
c. Detectives assigned to the case.
d. Identification personnel assigned to the scene.

Note: Supervisory, Command or any other personnel not involved in the investigation shall not be permitted in the crime scene.

4) The intentional alteration of the scene to conceal a crime, to stimulate a crime for personal reasons, to confuse or discredit investigators, or to steal incriminating evidence shall be prosecuted according to Section 4910 - Title 18 - CRIMES AND OFFENSES. § 4910. Tampering with or fabricating physical evidence. (2) makes, presents, or uses any record, document or thing knowing it to be false and with intent to mislead a public servant who is or may be engaged in such proceeding or investigation.

5) Deputies should be aware that inclement weather conditions may destroy or damage evidence.

B. The first deputy responding shall notify a supervisor, determine the jurisdictional authority, (with supervisory guidance) determine whether a major crime alert is required (via Everbridge), protect the entire scene, summon assistance from sworn personnel necessary to perform to perform the following duties:

1. Render first aid to the injured

   a. Where there are injuries, request ambulance through the PPD Radio M or T Band. If an injured person is lying down, outline the body position before removal, if possible.

2. If possible, question victim to find out who inflicted injury, what occurred and where (size and scope of the scene)

   a. Pay Particular attention to dying declarations and record:

      1) Name of victim
      2) Date, time, and location.
      3) Statement of victim-be as precise and accurate as possible.
4) Name of all other witnesses, both law enforcement and civilian.

3. A deputy shall notify PPD Radio M or T Band of updated conditions and request notifications be made to Command personnel, Detectives, Crime Scene Unit, Executive Staff, etc., if applicable).

4. If the PPD Radio M or T Band is unable to make said notifications, personnel at the ranking supervisor on-duty is responsible for such notifications.

   a. In the event the Sheriff is unavailable or cannot respond, the current call out list shall be utilized pursuant to the Directive on mandatory notifications.

5. Lawfully identify and detain all persons found at the scene.

   a. Get quick synopsis of crime and description of actor(s) from witnesses and victims for broadcast to other units if necessary.
   b. To prevent unnecessary conversation among witnesses, they shall to the extent possible, be separated from each other.
   c. Do not release anyone until cleared by a detective or the supervisor on the scene.

6. Arrest perpetrators found at the scene.

   a. Suspects will only be questioned by assigned detective.

7. Prevent anyone from touching or moving any object on the scene.

   a. A motor vehicle shall only be moved if it presents a hazard to public safety.
   b. If any object/vehicle is moved, outline its original position. In addition, record the exact original position and reason for movement. Give this information to the assigned detective or to the investigative unit supervisor.

8. File a written Incident Report and separate Crime Scene Log detailing of all actions and observations at scene. The record shall indicate:
a. Time of the establishment of the crime scene.
b. Time of police arrival
c. Names of all Sheriff/Police personnel who enter the crime scene.
d. Names of all persons present on arrival
e. Note any spontaneous statements/admissions.
f. All action taken and all observations pertinent to the case.

C. The first Sheriff’s Office supervisor on scene shall:

1. Initially decide what security is needed at the scene and decide whether to implement a major crime alert (Everbridge) or other of the City’s Emergency Operations Plans. The supervisor may modify as needed after consulting with responding Detective supervisor.
   
a) Determine the number of uniformed personnel required to protect the scene. Return all excess deputies to normal assignments.

2. Ensure that each deputy present files an incident report on actions and observations at scene.

3. Prevent anyone (deputy, police or civilian) from smoking, drinking, eating or any other activity which may detrimental to preservation and collection of evidence, to prevent contamination of the crime scene.

4. Stay at the scene and in command until officially relieved.

5. In situation where a deputy has discharged a firearm, personally check the weapons of each deputy present. Absent exigent circumstances instruct the deputy(s) to remove the magazine(s), if available. The deputy supervisor shall take possession of moved magazine(s) and make note of the number of remaining rounds.

D. The assigned IAD supervisor shall (in cases where the Sheriff’s Office is the primary investigator) shall ensure:

1. An IAD deputy deployed to the crime scene and that the deployed deputy takes command of the actual investigation. Since the IAD deputy will be involved in duties as an investigator, a Uniform Services (Criminal Division) shall remain in overall command of the crime scene protection
until the arrival of the IAD supervisor or until processing of the crime scene is complete.

2. Deputies preserve evidence by employing the best practices for evidence preservation and utilizing proper departmental equipment (e.g. bags, boxes, still and video cameras, casting materials, etc.).

3. A determination is made as to what evidence is sent to PPD Crime Scene Unit and ensures that the necessary forms are prepared and documented in the IAD electronic filing and case management system.

4. The collection and proper storage of evidence in order to preserve it and to maintain the chain of custody, by delivering it to the PPD Crime Lab-Evidence Custodian.

5. A Sheriff’s Office electronic case management report is completed/updated delineating the action taken at all scenes the IAD supervisor is called to process.

6. The collection of know samples, whenever possible, for comparison with unknown evidentiary items.

7. A crime scene sketch, when made, includes, but is not limited to the following:
   a. Measurements/dimensions of the scene.
   b. Relation of the scene to other fixed objects.
   c. Address, floor, room number and type of building (where applicable).
   d. Location of significant items within the scene to include the victim and all physical evidence.
   e. Any other item(s) deemed relevant to offense, scene, or situation.
   f. Direction of north.
   g. Sketcher’s name, date, and time of preparation.

8. Photographs are taken of the following at scenes where items of evidentiary value are found and collected:
   a. Overall scene including an exterior of the building if the scene is indoors.
b. All items to be collected or preserved prior to being moved.
c. All items which could be altered or destroyed in collection shall be
photographed with a scale prior to collection.

9. Mark evidence collected for later identification and ensures the Crime
Scene Unit Technician place her/his initials on all evidentiary items or on
the container, in the case of very small items.

E. The Uniform Services Supervisor shall:

1. Take command of the crime scene and consult with the PPD Patrol
Supervisor as to personnel needed.

2. Determine if additional personnel are needed to assist the assigned IAD
deputy.

   a. If conditions at the crime scene are unstable, determine whether
      firearms located on the scene should be immediately moved.
      Outline the original position prior to removal.

3. After completion of the crime scene processing, notifying Police Radio M
or T Band that Sheriff’s Deputies on-scene roles are complete, and units
are returning to service.

BY ORDER OF:

[Signature]

SHERIFF  DATE

185
DIRECTIVE: #30
SUBJECT: COMMENDATIONS
ISSUE DATE: 05-13-2020
REVISED DATE: 02-24-2021

I. POLICY:

A. Sheriff’s Office personal shall receive consideration for official recognition for outstanding performance during their duties as law enforcement officers or civilian employees.

B. Recommendations for recognition may be made by the Unit/Divisional Captain or above, or the highest-ranking civilian supervisor. Each of these requests shall be forwarded to the Sheriff via memorandum through the “Chain of Command”. Requests shall include the deputy sheriff’s or civilian performance evaluation for the current and past year and shall be endorsed through the chain of command as either as approved or disapproved, at all levels.

C. Official commendations are given to deserving personnel in recognition of an appreciation for outstanding acts of public service in the following:

1. Commendation for Valor (sworn only):
   
   a. For an extraordinary act of outstanding courage, without regard to personal safety, while in actual conflict with an armed and dangerous adversary.

2. Commendation for Bravery (sworn only):
   
   a. For the performance of an outstanding apprehension/arrest where the deputy’s effort is met by a dangerous adversary.
3. Commendation for Heroism (sworn only):
   a. For an act of heroism and outstanding courage without regard to personal safety, which results in the saving of a life.

4. Commendation of Merit:
   a. For an act of intelligent and valuable service, demonstration special faithfulness/perseverance including an especially important arrest/assist through highly intellect performance.

5. Commendatory Letter (sworn only):
   a. For an arrest or any service which is exception and beyond the requirements of routine duty.

6. Distinguished Unit Citation:
   a. Shall be awarded where the outstanding accomplishment is the result of team work rather than that of an individual.

7. Sheriff’s Letter of Recognition/Appreciation:
   a. The Sheriff’s Letter of Recognition/Appreciation shall be awarded for the performance of an employee, who in the opinion of the Sheriff or the Executive Staff has carried out an act or service that merits recognition above unit by the deputy’s chain of command.

II. PROCEDURES:

A. Commendation Recommendations:

1. Request for Commendations shall be submitted by the Unit/Division Captain or above (civilian manager) to the Sheriff, through the chain of command separate memoranda, in triplicate form for each case where a commendation is requested.

2. Requests shall be made as soon as possible after the incident occurs. In most cases. The submission of a request shall exceed thirty (30) days after the commendatory action has taken place.
3. The original and first copy shall be forwarded through the chain of command to the applicable deputy chief who, after review, evaluation, and recommendation as to appropriate from of commendation shall forward both copies to the Chief Deputy.

4. The second copy shall be filed in the employee’s personnel folder.

   NOTE: The captain or above (civilian equivalent) initiating the request shall forward an additional request to the captain or above (civilian equivalent) of all other participating deputies/employees.

B. When commendation recommendation is received from outside sources by way of letter or email, the communication shall be forwarded to the Chief of Staff, who shall ensure distribution shall be the same as delineated in above sections in this directive.

C. Descriptions of all approved uniform commendations are contained in Directive 4.
DIRECTIVE: #31
SUBJECT: WELLNESS UNIT
ISSUE DATE: 01-16-2020
REVISED DATE: 02-24-2021

1) PURPOSE:

The purpose of this directive is to provide personalized support for Sheriff's Office members by diminishing or eradicating obstructions to employee wellness, whether personally or professionally induced, through intervention, training, and access to wellness assistance resources.

2) POLICY:

A. The Philadelphia Sheriff's Office recognizes that commanders and managers are the primary caregivers to the people they supervise and have a duty to ensure their wellbeing. To realize this belief the Philadelphia Sheriff's Office has created the Sheriff's Office Wellness Unit, which serves as a wellness resource for Sheriff's Office staff to intervene in employee crisis incidents, training staff on how to maintain their own wellness and how to help others to do the same and finally make Sheriff's Office staff aware of wellness help resources available within the Philadelphia community.

B. The Sheriff’s Office Wellness Unit shall consist of the Philadelphia Sheriff’s Office Traumatic Incident Coordinator, Sheriff’s Office sergeant, the Sheriff’s Office chaplain, a deputy, and a civilian employee. The senior sergeant shall serve as the Commander of the Wellness Unit, with guidance from the Traumatic Incident Coordinator. Recruits to the Wellness Unit shall be compassionate, non-judgmental, experienced within the Sheriff’s Office, trustworthy and respected by their colleagues. The assignment is completely voluntary. Commanders and managers shall choose staff within their units
that they believe, are suitable to staff the Wellness Unit. The Sheriff, the Chief Deputy and Chief of Staff shall choose from among the candidates selected by the commanders and managers via interviews and resumes. Commanders and managers can only select employees, who are in good standing. Chaplains shall be chosen by the Sheriff, exclusively. Every member of the Well Unit shall serve in the unit for a term of two (2) years, except for the Traumatic Incident Coordinator, who serves as a permanent member.

C. When employees are directed to or voluntarily seek assistance from the Wellness Unit, only the supervisors and/or commanders with the need to know can be informed of such occurrences. All Wellness Unit personnel shall sign a confidentiality/non-disclosure contract with the Sheriff’s Office. All communication rendered by Sheriff’s Office personnel to the Wellness Unit staff shall be covered under the confidentiality/non-disclosure agreement except for the following:

1) If the employee is a danger to her/himself or to others.
2) If there is suspected child abuse.
3) If there is suspected domestic violence or fear thereof.
4) If there is suspected elder abuse or abuse of incapacitated persons.
5) Narcotics offenses or usage on duty.
6) Felonies
7) Felonies committed on duty
8) Matters that would jeopardizes the safety of the public.
9) When staff receiving wellness services requests in writing that her/his given information be shared with Wellness Unit Commander.

NOTE: All parties involved shall be made aware that statements made to the Wellness Unit are not considered privileged and are subject to subpoena and other legal discovery.

D. Deployment:

1) The Wellness Unit personnel shall be on call twenty-four (24) hours per day and seven (7) days per week.

2) Wellness Unit staff shall not only be on location at Sheriff’s Office facilities but shall also meet with employees seeking help at the times and locations that work best for employees.
3) The Commanding Officer of the Wellness Unit shall authorize deployment of Wellness Unit staff to crisis/traumatic incidents and does not have to wait for authorization from Command Staff to do so. The Wellness Unit Commanding Officer shall notify the Chief Deputy and Chief of Staff of very deployment.

4) Wellness Unit Staff shall regularly check with the employees who use their services and follow up on anniversary dates of critical incidents as well.

5) The Wellness Unit is responsible for the establishment of a peer support group, consisting of sworn and civilian employees. Peer support group recruits must exhibit the following characteristics:

   a) Compassionate
   b) Non-judgmental
   c) Experienced in the Sheriff’s Office
   d) Trustworthy
   e) Respected by colleague

6) The Wellness Unit Commander shall be responsible for the maintenance of an accurate roster of names, telephone numbers, duty assignments and other important information regarding the availability of Peer Support Team members, who may respond to assist in critical/traumatic incidents.

7) Upon request by Command Staff, the Wellness Unit Commander shall authorize a Peer Group Team member to intervene during a disciplinary action, on the behalf of any Sheriff’s Office employee to determine if the root cause of an infraction is of an emotional or psychological nature.

8) A Peer Group Member may be allowed to accompany a Sheriff’s Office employee through all phases of investigations, involving the employee. The Peer Member’s status is not official, and the member shall take no part in the investigation. Under no circumstances should the Peer Group member do anything that may interfere or disrupt an investigation.
9) All Peer Group Members shall be under the same confidentiality/non-disclosure agreements as the Wellness Unit.

10) Neither Peer Support nor the Wellness Unit shall be used for sworn duties when they are off-duty and acting in the capacity of Peer Support or crisis/traumatic incident intervention.

3) PROCEDURE:

A. The Commander of the Wellness Unit shall ensure that every member of the Wellness Unit and the Peer Group receive Crisis Intervention Team training, Trauma Informed Customer Service training, and Peer Group Facilitator and Peer Support training.

B. The Sheriff’s Office Wellness Unit shall provide the following services:

a) Healthy Nutrition/Healthy Eating
b) Physical Fitness
c) Health Self-Assessment
d) Stress Reduction
e) Criticism response management
f) Mindfulness Training
g) Healthy Lifestyles
h) Healthy Sleeping Habits
i) Biofeedback
j) Trauma Resiliency Training
k) Employee Assistance Program (EAP) referrals
l) Conduct Critical Incident Debriefings
m) Suicide Prevention Counseling

C. The Commander of the Wellness Unit shall ensure that every member of the Unit prepares an activity log for daily scheduled assignments for Peer Support Group she/he is assigned to facilitate. Each completed assignment shall be recorded in the activity log along with the number of employees that participated in the activity. At the end of each activity or training, a survey shall be presented to the participants to serve as a metrics for success. At the end of the month, all unit activity shall be tallied, and the surveys calculated to determine what services were rendered and how they were received by the participants. A final yearly tally shall be published on the Sheriff’s Office website.
D. Wellness Unit members shall keep updated and orderly files, containing crisis/traumatic incidents, service recipients names, activities conducted, dates, starting and ending times and location of activities.

E. Wellness Unit members shall follow the subsequent procedures for all service recipient intakes:
Via Phone:

1) The Wellness Unit members shall allow service recipients who place calls to the Wellness Unit to vent before obtaining their personal information. Cutting the persons off to acquire personal information may stop the person from talking. When an appropriate break in the conversation occurs, personal information shall be obtained at that time. The information collected shall include:

   a) The service recipient’s name
   b) Title
   c) Work facility/Unit
   d) Address
   e) Phone number
   f) Date and time
   g) Nature of the service request
   h) Follow up recommendations

2) The service recipient shall be assigned a file case number.

3) The follow up session shall be scheduled as soon as possible. The service recipient shall determine if the next service take place in the Wellness Unit or at another location.

   NOTE: Wellness Unit Staff are on call 24/7. When called into service during off-duty hours, Wellness Unit personnel shall contact the Wellness Unit Commander once the service is completed.

Walk-ins:

1) Service recipients who walk into the Wellness Unit for service shall be triaged as soon as possible to ensure that service recipient does not back out of seeking help. The triage service provider shall obtain personal informal form the recipient of care.
2) The Service recipient shall be assigned a case file number and a follow-up appointment date as soon as possible.

Critical Incident Response:

1) All Wellness Unit responses to critical incidents, such as deputy involved shootings, employee deaths, etc., shall be dispatched by the Wellness Unit Commander. The Unit Commander shall log the incident, the staff involved, and the Wellness Unit personnel dispatched to the scene. If multiple incidents occur, the Wellness Unit Commander may authorize a Peer Support Team to be deployed to the incident.

2) Once on the scene of a critical incident, Wellness Unit staff shall adhere to the following protocols:

   a. Assess the impact of the critical incident on support personnel and incident survivors.
   b. Identify psychological and emotional issues surrounding problems of safety and security.
   c. Use calming by allowing for the airing out of thoughts, emotions and experiences associated with the event and validate the responses of those impacted by critical incidents.
   d. Try to foresee the consequences of the event and prepare for the emotional and psychological impact of these consequences.
   e. Conduct a “Systematic Review of the Critical Incident” and its’ impact emotionally, cognitively and physically on the survivors and support personnel. It should be noted this is not a critical review of the incident, but it is only conducted to provide emotional and psychological support to the responders and survivors of a critical incident.
   f. Bring closure to the event. Ground the survivors and support personnel to community resources, with back up provided by the Sheriff’s Office Peer Support Group to initiate the processes of “moving on”. If possible, point out any good achieved from the critical incident.

F. The Wellness Unit Commander shall oversee Peer Support Group. The Wellness Unit Commander shall serve Peer Group Facilitator and shall ensure
the following protocols shall be adhered to during Peer Support Group sessions:

1) Time shall be allotted to Peer Group members sharing their previous weeks' challenges and successes.
2) Encourage feedback from last session to receive critiques, clarify any misunderstandings and wrap up any unresolved issues.
3) Do a Mood Check by conducting a survey as to how individual members of the support group are feeling.
4) Perform a review of Homework assignments. The public review of homework assignments stresses the importance of the practice of healing techniques between sessions.
5) Set an agenda for the current session and ensure that all members know the psycho-educational topic for the session.
6) Establish goals. Each member of the support group shall establish a goal to be achieved during the session.
7) Use a quick self-test so that members of the support group can gauge their understanding of the session topic.
8) Take a mindful minute to think about the session’s topic and as you use breathing exercises, visualization, and guided imagery to allow support group members to focus on the session’s subject in a more mindful way.
9) All activities and number of participants shall be logged by the facilitator and kept to files, which shall be tabulated for end of the year issue on the Sheriff’s Office website.
Philadelpbia Sheriff's Office

DIRECTIVE: #32
SUBJECT: ARMORY: WEAPONS, AMMO, & FIREARMS
ISSUE DATE: 04-08-2020
REVISED DATE: 02-24-2021

I. PURPOSE:

A. The purpose of this Directive is to establish a set of standards governing the management of the weapons armory and storage of confiscated or surrendered firearms received by the Philadelphia Office of the Sheriff. The directive aligns with laws set by statute in the Commonwealth of Pennsylvania for Elected Sheriffs.

B. The Office (or Department) recognizes the sanctity of all human life and is committed to respecting the dignity of all persons. The primary duty of all Deputy Sheriffs is to preserve human life; this extends to and applies to our policy on the safe storage and disposal of weapons, firearms, and ammunition.

C. In October 2018, the Pennsylvania Governor signed into law Act 79 of 2018, which made changes to the PA Uniform Firearms Act and the PA Protection from Abuse Act. The Act went into effect on April 10, 2019, and modifies the procedures regarding the relinquishment of firearms, ammunition and other weapons by the defendant named in a Protection from Abuse Order (PFA), or an individual who is convicted of a Misdemeanor Crime of Domestic Violence.

D. This legislation also affected the issuance of a Pennsylvania License to Carry Firearms and changed the Pennsylvania Uniform Firearms Act (18 PA C.S.).

II. POLICY:

A. The policy of the Philadelphia Office of the Sheriff is to maintain an Armory for the storage of firearms (long guns and handguns) classified as approved weapons for use and issuance to sworn members of the Department.

B. It is the policy of this Office to accept any relinquished weapons pursuant to law.
C. It is also the policy of the Sheriff to accept firearms, weapons, and ammunition for storage in the armory without question. A person surrendering a firearm, weapon, or ammunition may relinquish any of the same anonymously.

1. Firearms relinquished voluntarily shall remained stored in the Sheriff’s Office Armory.

2. Firearms, weapons, and ammunition relinquished voluntarily OR that remained unclaimed at least 1-year post Act 79 court ordered adjudication are considered abandoned and become property of the Philadelphia Office of the Sheriff.

3. Firearms that become property of the Office of the Sheriff under II, C-2 shall be submitted to the Philadelphia Police Department Firearms Identification Unit for NIBINS testing by the Firearms Technician on the date of surrender, and after 5pm, the next business day.

D. Effective April 10, 2019, PA Act 79 resulted in the following changes:

1. Required changes to forms commonly used by PA Federal Firearms Dealers.

2. Firearms, ammunition, and other weapons can no longer be given to friends or family for PFA third-party safekeeping.

3. Firearms, ammunition, and other weapons can be relinquished to a Sheriff’s office, law enforcement agency, a Federal Firearms Dealer, or a licensed Commercial Armory.

4. Firearms, ammunition, and other weapons must be relinquished within 24 hours of the issuance of a final PFA or the service of a temporary PFA, unless the court orders otherwise.

E. The Office of the Sheriff Armory shall also serve as the official storage area for Act 79 surrendered weapons, ammunition and firearms relinquished into the custody of the Office of the Sheriff.

1. All relinquished weapons, firearms, and ammunition pursuant to court order or voluntarily surrendered to the Office of the Sheriff under Act 79 will be stored in the Armory.

2. **Access:** In order to prevent the alteration, unauthorized removal, theft, or other compromise of property stored by the Office of the Sheriff, and to maintain the chain of custody, only selected and authorized individuals will have key access to the armory.
a. Sworn members of the Office of the Sheriff of any rank will present their unexpired Sheriff Department (Police Department, or City of Philadelphia Office of the Controller) identification card to the Firearms Technician who will log the visitor into the armory using the Armory Firearms Weapon and Ammunition room log book. This entry will indicate:

1) The date of access.
2) The time in:
3) The incident/case number, and the item/property receipt number(s) being sought, removed, or returned.
4) The Deputies moving the items in or out.
5) The reason for entering, i.e., depositing items for storage, removing items to return to owner's, item(s) for destruction, etc.; and
6) The time out.

3. The Armory will have a secured and physically segmented area serving as intake, storage area, and distribution point for all firearms, weapons and ammunition purchased for use by the Office of the Sheriff.

4. Evidence Storage: All weapons, narcotics and evidence seized pursuant to arrests will be processed by the City of Philadelphia Police Crime Lab as Evidence Custodian and stored at the Firearms Unit and Crime Lab/Forensic Science Facility located at 8th& Poplar.

F. The Sheriff's Office will designate the Deputy Chief of Training as the Office of the Sheriff Firearms and Weapons Custodian and charges the Deputy Chief with the responsibility to assign Firearms Technicians to maintain the Armory as a secure temporary evidence/property storage/ weapon issuance facility in the Land Title Building 5th Floor located at 100 S. Broad Street, 5th Floor.

1. The Deputy Sheriff accepting a relinquished weapon, ammunition or firearm shall:

a. Enter the property into the Property Receipt logbook available at all Uniformed Services Sheriff facilities where weapons are surrendered.
b. Place the item(s) on a property receipt (specifically noting if weapon is a court ordered surrender).
c. Categorize all firearms, as handguns or long guns.
d. Secure the firearm with a zip tie (as illustrated in Attachment A).
e. Make the weapon/firearm safe, if necessary, contact the Police Department SWAT Unit to disarm a loaded firearm or firearm-like weapon.
f. Add the make model and serial numbers of items, if legible, and other distinguishing characteristics of the item(s) on the property receipt.
g. Sign and accurately date the property receipt, adding the payroll number of the deputy accepting the weapon, ammunition, or firearm.
h. Scan the item into our custody via the Teleosoft-Armory software package and affix the applicable barcode sticker.
2. The Deputy Sheriff Supervisor shall:

a. Ensure the property is logged into the Property Receipt Logbook and (at a minimum) that all items listed in this directive (from II-A-1, a-h) are described, secured, unloaded, and labeled pursuant to this directive.
b. Act as the witness by endorsing the property receipt.
c. Notify the Firearms Technician and Deputy Chief of Training (via email cc) that items requiring storage in the Armory are ready for transport from their location.
d. Ensure that prior to authorizing the deployment or use of any weapon, handgun, firearm, long gun, etc. that a Firearms Technician has received the appropriate training enabling the Firearms Technician to safely handle the instrument.

3. The Firearms Technician will:

a. Ensure that prior to deploying or handling any weapon, firearm, long gun, shotgun, rifle, ammunition, etc., the deputy being issued the instrument has received the appropriate training enabling the safe use and handling of the instrument.

1) Shall be PCCD certified or achieve certification via PCCD certified trainer, in the use of the weapon, firearm, long-gun.
2) Shall be PCCD certified or achieve certification via PCCD certified trainer to train deputies in the safe use of the weapon, firearm, long-gun, etc.

b. Work as the department Armorer and Firearms Trainer; reporting under the Training Division Lieutenant.

1) The Training Division Deputy Chief or Training Division Inspector may train and designate deputies as Firearms Technicians.
2) The Training Division Chief will not serve as an Armorer or Firearms Technician and will ensure that a minimum of two (2) sworn Firearms Technicians and one (1) supervisor are always trained to serve in that capacity.

c. Ensure entry of the item(s) into the Teleosoft Armory software package, check for the prerequisite bar code, and cross check the information on the property receipt with the items submitted for accuracy.

d. Maintains a current location and accurate inventory of all Department-owned firearms, from initial possession to final disposition in the Teleosoft Armory.

e. Takes all reasonable steps to ensure the security of firearms stored at the Armory facility.
f. When placing a firearm into service, physically inspects each weapon and records the make, model, and serial number into the Teleosoft Armory database.

g. Maintains responsibility for all Department-owned firearms that are to be destroyed except firearms that are evidence.

h. Transport the zip tied, unloaded secure weapon, firearm, or ammunition from the Office of the Sheriff facility where the property was accepted to the armory.

i. Log the item(s) via barcode into the custody of the Armory using the Teleosoft software package in an orderly and easily searchable manner, in a location within the armory consistent with the information logged into the evidence software system.

j. Will maintain a secure and monitored storage area that is separate from all confiscated or surrendered weapons, handguns, long-guns, and ammunition that houses unissued Office of the Sheriff owned handguns, long-guns, and weapons. Ammunition in all cases will be stored separately (at all times).

k. Determine if weapons, firearms, or ammunition stored in the armory are held in a manner consistent with court orders and/or orders of destruction.

1. Items beyond the statute of limitations shall be returned to the owner, if possible.

2. Through the Firearms Technician, owners will be sent at least one communication from the Sheriff via registered mail to their last known address.

3. A record of the attempt to contact via registered U.S. Mail will be maintained by the Firearms Technician in the logbook and Teleosoft Armory software package.

   a. Ensure property stored in the armory will be kept in a neat and organized manner, and/or disposed of in a manner consistent with PA statutory law.

      1) The Firearms Technician will witness and record the destruction of weapons pursuant to PA statutory law.

4. When employees issued firearms are retiring or separating, the employee will surrender all individually issued firearms to the Firearms Technician who will ensure the Training Captain updates the training records.

G. Inspections / Audits
1. Inspections of the Armory aid in ensuring the integrity of the control systems and security of all items stored therein.

   a. All Uniform Operations Supervisors working any day after 5p and before 8a, shall make at least one unscheduled physical daily check of the exterior security of the Armory at 100 S. Broad Street, 5th floor.

   b. The Uniform Operations Supervisor will enter the prerequisite information in the Armory logbook to confirm the Armory check.

   c. If the book is missing the supervisor will make an incident report and log the check in the body of the report and forward copies of the report to the IAD Deputy Chief and the Chief Deputy for investigation and video review.

      1) The supervisor will make a City of Philadelphia Police Department report to Central Detective Division immediately.
      2) The supervisor will notify the Chief of Staff and IAD on call investigator.
      3) A Firearms Technician will be called in to review the video and provide access to the videotaped areas to the PPD assigned investigator and PSO-IAD.

2. Control systems are necessary for the following reasons:

   a. To ensure the area is maintained in a safe, clean, and professional manner.

   b. To ensure that the integrity of the property within the armory is being satisfactorily maintained.

   c. To ensure the provisions of Sheriff Office directives regarding weapons, firearm, and ammunition safety are being followed.

   d. To ensure that items secured in the armory are being protected from theft, damage, and deterioration.

   e. To institute and enforce accountability procedures are being maintained; and

   f. For adherence to the proper and legal cycle of disposal of items surrendered or relinquished into our care.

3. An “audit” is a random occurrence that determines adherence to procedures used for the control of property. The Deputy Chief of Training will ensure a random audit is conducted at least one time per quarter is performed by the Deputy Chief of Training, City Controller, or their designee.

   a. An “inventory” of property in the Armory will occur before 12/31 of each year AND whenever the Training Division Deputy Chief and/or Firearms
Technician is assigned to and/or transferred from the position. The inventory will be conducted jointly by the newly designated Firearms Technician, Deputy Chief of Training, Sheriff, or his/her designee to ensure that records are accurate, secure, and properly annotated.

b. An inventory requires that all firearms and weapons that cannot be accounted for must be reported on a PSO Incident report AND to the Philadelphia Police Department.

c. Also, as a best practice, the Chief of Staff will ensure that Telesoft-Armory permissions of the transferred employee are reduced, codes from alarm panels and video access will be changed, keys will be returned, and if needed (or applicable) combinations will also be changed.

d. As an additional check and balance, a supervisor and the Chief of Staff will conduct a quarterly audit of property held in the armory and any off-site location(s).

1) The audits shall be random, and a sampling generated by the Armory-Telesoft Database of all property held, to memorialize the procedure and to satisfy the auditor that policies and procedures are being followed.
2) Off-site locations should have minimal issued weaponry (i.e., shotguns used by the Transportation Unit and rifles at CJC-Garage and NE Parking Area-Safe), therefore a total inventory of all weapons will be conducted at those locations to include ammunition in every audit memorandum.

e. The Firearms Technician shall video control system audits of the armory on the first and last day of each tour of duty. The audits shall primarily review times when the armory was unattended and shall be a minimum of eight (8) total footage reviews of a minimum of four (4) hour increments.

1) The video audit shall be memorialized via memorandum to the Chief of Staff and shall capture dates, times, and person reviewing video footage.
2) The Firearms Technician/auditor shall include their PR# and signature to certify the audit was conducted.
3) As an additional check and balance, if the Firearms Technician/Auditor finds that overnight supervisors have been negligent in checking the security of the armory during off-hours, they will prominently indicate that information in the memorandum, to ensure proper corrective actions can be taken.

f. The City Controller or their designee may request an audit of property and / or video in the armory at any time. The Firearms Technician or Deputy Chief of Training shall facilitate the audit process without unnecessary delay.
G. Status of Property: The current status of all items stored in the Office of the Sheriff Armory will be reflected in the following records:

1. Armory-Teleosoft database/software; and
2. Bar coding system

H. Removal of Stored Property

1. Under no circumstances will property relinquished or surrendered pursuant to PA Act 79 or used to equip or train sworn members of the Sheriff’s Office be taken from the armory for personal use by any person, regardless of rank or position, from either within or outside the Office of the Sheriff.

2. Any request to review vaulted items will be submitted to the Deputy Chief of Training to coordinate a date for the review.

3. All audits or inventories will take place within the armory with a Firearms Technician present the entire time during the review.

4. Occasionally items will be transferred to another agency (i.e., the District Attorney’s Office, ATF, FBI, or the Philadelphia Police Department). Upon return to the Armory all items will be inventoried, and cross referenced with the property receipt by the Firearms Technician in the presence of the returning law enforcement officer.

   a. When possession of an item is transferred from one person to another, a record will be made of the transfer by printing the Armory Teleosoft barcoding receipt and inserting that receipt into the file/area where the item was removed.  
   b. The record of transfer applies to all persons, functions, and components within the Office of the Sheriff and outside agencies.

   c. The printed form shall include:

   1) The PSO Case/Incident number.
   2) The agency of origin.
   3) The Agency case number.
   4) The name and agency (badge or payroll number, if applicable) of the person releasing the item.
   5) The name and agency (badge or payroll number, if applicable) of the person receiving the item.
   6) The property receipt number
   7) The date of transfer; and
   8) The time of transfer
I. Disposition

1. A final disposition of the status of any item secured as a result of surrender or relinquishment pursuant to PA Act 79 will be made after legal requirements have been satisfied. The prompt, legal authorized disposition of property/obtainment of a destruction order prevents an overload on the Armory-Telesoft tracking/barcoding database, reduces the requirements for additional space and allows owners to reclaim their items in an orderly manner.

2. Quarterly, a prepared list will be reviewed by the Deputy Chief of Training and the Evidence Technician for the purpose of determining which items in the armory can be purged and to determine a final appropriate legal disposition.

3. Prior to destruction of any firearm, weapon and/or ammunition:

   a. A correspondence letter will be sent to the last known address listed on the property receipt with informing the owner at least 30-days to prior scheduled destruction.
   b. If the owner fails to physically claim the item prior to the date of destruction, the firearm, weapon, or ammunition will be prepared for destruction and:

       1) The weapon will be tagged, and zip tied.
       2) A list will be created of all weapons to be destroyed.
       3) The list will be verified to include all weapons to be destroyed by a minimum of two (2) Firearms Technicians and a Supervisor.
       4) All containers upon verification of weapons AND the list, will be secured via a lock.
       5) On the Date of destruction, an IA Officer/Supervisor will re-verify the accuracy of the list in the presence of the Firearms Technician and Supervisor, and all containers will again be secured.

c. A list of weapons to be destroyed will be provided to enable a neutral third party to audit firearms, weapons, and ammunition at the destruction site.

d. All firearms, weapons and ammunition will be destroyed alongside PPD Evidence Unit to witness the destruction.

1) Witnesses to the destruction of firearms, weapons, and ammunition shall be recorded via entry into Telesoft by the Firearms Technician assigned to the destruction.

BY ORDER OF:

[Signature]

SHERIFF DATE

204
DIRECTIVE: #33
SUBJECT: SELECTION AND TRAINING
ISSUE DATE: 05-12-20
REVISED DATE: 12-19-2020

1. PURPOSE:

A. The purpose of this directive is to align Philadelphia Sheriff’s Office personnel performance with our mission and values. As we endeavor to establish a workforce that is the embodiment of integrity, honor, and service, we realize this goal shall only be attained through the proper recruitment, training, and development of personnel. The process of training and development cannot begin until the best candidates for the position of deputy sheriff have been selected. This statement is made with the full understanding that the term best candidates must be broader than the traditional view of what it meant, historically. The movement from the warrior model of law enforcement to the guardian model of law enforcement means that we must seek recruits who best exhibit the characteristics of the guardian model of law enforcement. These characteristics are the building blocks upon which continual training and development lead to success and excellence.

2. POLICY:

A. It the policy of the Philadelphia Sheriff’s Office to organize and administer the Office’s training component in a manner, which is responsive to the operational task requirements of the agency, its personnel, and the community it serves. Training and Development shall focus on subjects of education and instruction which will develop knowledge, skills, and abilities related to job task requirements and community expectations. Documentation of training activities shall be maintained, and requirements for developmental and remedial training will be monitored and implemented in accordance the procedural elements of this policy.

B. All Office training shall be in compliance with the Sheriff and Deputy Sheriff Education and Training Act (PA Title 71 section 2105) regarding deputy sheriff training and agency responsibilities including:

1. Educational prerequisites are established by statute (see: Sheriff and Deputy Sheriff Education and Training Act) No persons shall be hired as a deputy sheriff,
who has not obtained a high school diploma or has received a secondary school diploma on the basis of general education development (GED) (see: Sheriff and Deputy Sheriff Education and Training Act).

2. Physical fitness standards prior to employment are set by the Training and Educational Services Bureau (TESB) with the approval of the Sheriff. Once the recruit is hired and enters the Sheriff and Deputy Sheriff Basic Training Academy all standards are set by the Pennsylvania Commission on Crime and Delinquency (PCCD).

3. All Sheriffs and deputy sheriffs within the Commonwealth must complete the process of PCCD certification within one year of hire date.

C. All Sheriff’s Office personnel, sworn and civilian, shall attend designate mandatory and in-service training, which may include materials on Federal and State legal updates.

D. All Sheriff’s Office personnel, sworn and civilian shall attend training appropriate for their assignment. Attendance at training is considered a requirement of the assignment.

3. Selection of Personnel:

A. Recruitment and Selection

1. The current standards and hiring criteria for the Philadelphia Sheriff’s Office is as follows:

   (a) The Philadelphia Sheriff’s Office Recruit Training Unit (RTU) shall ensure that all recruits/applicants are made aware that they are required to successfully complete the Deputy Sheriff Certification Training conducted by the Pennsylvania Commission on Crime Delinquency (PCCD) to become certified deputies. The aforementioned is a 2-week -19-week course which requires the recruits to attend The Pennsylvania State University in State College, PA.

   (b) RTU shall ensure that all recruits/applicants, who live outside of Philadelphia County, know if they successfully complete the Sheriff’s Office background investigation and hiring process, they have six months to move into the City and County of Philadelphia from their date of hire. The RTU shall have every recruit to sign an affidavit attesting they shall in fact move into the jurisdiction within the prescribed timeframe.

   (c) All applicants must have achieved a high school diploma or GED

   (d) All applicants must possess a proper class driver’s license issued by any State in the United States of America prior to appointment and must obtain a proper class valid driver’s license issued by the Commonwealth of Pennsylvania within 6-months of appointment.
(e) All applicants must complete the following:

- Employment Application
- Pass written examination
- Physical Agility Test
- Personnel Data Questionnaire (PDQ)/ Interview
- Drug-Screening Test
- Medical Evaluation Physical
- Psychological Evaluation
- Hiring Panel Evaluation
- Indebtedness-Check

(f) All applicants must complete a Personal Data Questionnaire (PDQ) booklet within the timeframe announced by RTU.

(g) All applicants must pass a complete background investigation, physical agility test and physical and psychological examinations. The RTU shall make the recruits/applicants aware that if they successfully complete the background investigation and hiring process, a secondary Physical Agility Test is required, upon matriculation into Deputy Sheriff Training Academy. Failure to do so could result in termination.

(h) All applicants shall be examined by a hiring panel. The panel shall be charged with the determination status. It shall be noted that the Sheriff has the final say in the decision to hire.

(i) The Background Investigator and Hiring Panel must take a deeper look at the applicants. All Sheriff’s Office members involved in the hiring process shall keep in mind that the goal is to hire people who share our values as a public office. In other words, we shall make every effort to hire people, who meet our criteria as to what characteristics a Philadelphia Sheriff’s Deputy should have. Among, the characteristics to be considered are:

- Integrity
- Service Orientation (Community Involvement)
- Empathy
- Communication and Human Relation Skills
- Self-Control
- Team Orientation
- Problem Solving Skills

4. Training Procedures:

A. Training and Education Services Bureau

1. The Training and Education Service Bureau (TESB) operates and maintains the following Units:
a. Recruit Training Unit (RTU)
b. Advanced Training Unit (ATU)
c. Firearms Training Unit (FTU)

1. Recruit Training Unit (RTU) shall be responsible for but is not limited to instruction on the following subjects:
   a. Philadelphia Sheriff’s Office history and mission
   b. Principles and history of law enforcement
   c. Ethics and Moral Issues
   d. USE of Force
   e. Community orientated law enforcement and problem solving
   f. Court room and detention area security
   g. Report Writing
   h. Implicit bias training
   i. Search and seizure
   j. Constitutional law
   k. Procedural Justice
   l. Civil law
   m. Domestic violence (PFA)
   n. Mental Health
   o. Firearms
   p. Handcuffing
   q. Pepper spray (OC)
   r. Tactical First Aid

2. RTU shall assign each facility with a Training Deputy (Field Training Officers) to reinforce training practices and principles consistent with policy. This will ensure recruits are prepared for enrollment into the Deputy Sheriff Academy.

3. ATU is responsible annual training (ACT-II- 2014) for all certified deputies. This pertains to scheduling and administration of all PCCD Continuing Education in-service training. ATU shall locate and identify advanced and specialized trainings/schools for deputies. ATU shall coordinate with the Unit Commander of all training for approval and/or designee.

   a. All Unit Commanders shall perform a training audit for their unit and submit the findings to their Deputy Chief and/or designee Upon approval, ATU will schedule the appropriate training.

4. FTU is responsible for training all deputies and recruits in the proper handling and safety for firearms. FTU shall prepare written materials and conduct practical drills to ensure familiarization firearms and drill techniques.

5. Citizen’s Sheriff’s Academy
ATU shall establish an accelerated civilian training program for purposes of teaching members of the community about the policies and procedures of the Sheriff’s Office, the laws and statutes which dictate deputy behavior and the structure and limits of the power of the Sheriff’s Office. Community members who successfully complete this training shall be eligible for a position on the Philadelphia Sheriff’s Office Community Advisory Board.

6. Unit Training

The Commander of each unit shall ensure that deputies are trained and knowledgeable of facility policy and Standard Operating Procedures (SOP). Failure to train and teach is a failure to supervise. All SOP’s have to be submitted to, reviewed, and approved by the Chief Deputy. Unit Commanders must annually review SOP’s and submit to the Chief Deputy.

7. Internal Affairs

The Unit Commander and the Undersheriff shall ensure that upon transfer to the unit and prior to conducting an Internal Affairs Investigation shall prescribed training, as per office policy—Upon completion of introductory training, all records (sign-in sheets, lesson plan, test scores, etc.) are sent to ATU for entry in the deputy’s training record.

8. Supervisory Training and Management Development

As deputies and civilians are promoted the change of their roles within the Office, demand that they acquire supervisory, management and administrative skills. The Sheriff’s Office shall ensure that deputies are provided the appropriate training according to their future rank prior to being promoted. Pre-promotion training will be scheduled by ATU for in-service or out-service training, based on the position held or future promoted—Training may include, but not be limited to the following:

- National Credible Leadership Certification-conducted by the National-conducted by Sheriff’s Association and the National Command and Staff College.
- Jail Evacuations-conducted by the National Sherriff Association and the Department of Homeland Security.
- Court and Judicial Security Certification-conducted by the National Sheriff’s Association and Texas A&M.
- Police Supervisor In-Service Training Institute (POSIT/POLEX)-conducted by Penn State’s Criminal Justice Program.
- FBI- LEEDA National Academy
- Court Security Assessment-conducted by National Sheriff’s Association.

209
5. Remedial Training

a. Remedial Training is individualized instruction used for specific deficiencies in personal job performance. Generally, the need for remedial training is recognized during following activities:

1. Supervisory evaluation (i.e. observation of rudimentary job performance)
2. Review of duty-related auto accidents
3. Review of critical incidents
4. Training

b. A determination that any aspect of an employee's duty-related responsibilities is deficient may serve as the reason for requiring remedial training.

c. Commanding Officers shall require any employee under their command to receive remedial training when it has been determined that the employee has violated any departmental policy, Directive of Sheriff's Memorandum, has failed PCCD in-service training, or may otherwise benefit from remedial training.

(1) Remedial Training shall be administered through these procedures:

a. Submission of Training Request Memorandum through the chain of command to the Deputy Chief in charge of Training and Educational Services Bureau.

b. Direct issuance of a reprimand or statement of charges to an employee, who would then be scheduled by the Training and Educational Services Bureau for remedial training.

c. Training which could be done at the unit level shall be conducted by a supervisor and results of such training shall be submitted to the TESB.

d. Employees who are scheduled for remedial training are required to attend. An employee’s failure to report to, participate in or complete the training shall be documented via memorandum through the chain of command to the Deputy Chief of TESB and may result in disciplinary action.

e. Remedial training shall be documented by TESB and the employee’s Commander shall be notified of the progress and/or outcome of such training.

f. Personnel unable to exhibit proficiency or qualify with any authorized weapon shall receive remedial training from FTU; after the third attempt of annual qualification, the deputy is subject to termination.

6. Mental Health Training

A. The Sheriff's Office shall ensure that all personnel receive initial training to recognize and respond to suspected mentally ill persons.
B. The Sheriff’s Office shall provide training in any area of mental health awareness at least once three (3) years. This training shall be administered in a manner determined by TESB.

C. The Sheriff’s Office shall provide Mental Health training within 90 days of any changes in mental health statues or Sheriff’s Office policy.

D. All deputies shall receive Crisis Intervention Training (CIT) and shall receive refresher training every two (2) years.

12. Fair and Impartial Law Enforcement, Procedural Justice

The Sheriff’s Office shall provide initial and re-training on Office policy and implicit and overt bias-based law enforcement issues once every three (3) years.

13. Non-Mandatory Training for Sworn Personnel

Request for non-mandatory training will be submitted through the chain of command.

14. Mandatory Training for Non-Sworn Personnel

A. Newly appointed civilian employees shall receive an orientation training program introducing them to the Philadelphia Sheriff’s Office. The orientation program shall be coordinated by Human Resources and TESB and at a minimum shall include:

(1) The Sheriff’s Office role, purpose, policies, and procedures.
(2) Working conditions, rules, and regulations.
(3) Rights and Responsibilities of employees

B. All newly hired non-sworn personnel shall receive training appropriate for their duties. Training shall be documented by the employee’s Unit Commander and the TESB.

C. In-Service training designed specifically for non-sworn employees shall be conducted as available and necessary.

(1) Training shall be designed to review and update current duties, and skills, as well as, to train and inform the employee of new responsibilities or serve as career development training.

15. Career Development/ Personnel Training

A. Management and supervisory training are a major factor in enhancing an employee’s overall potential for positions of leadership, therefore the Philadelphia Sheriff’s Office shall not wait until promotions are made or certifications are due to provide training for deputies. As every deputy is a
supervisor in some way, whether it’s directing the public in the courthouses or prisoners on the cell block, all deputies are responsible for supervising someone and should be provided training for career enhancement.

B. The TESB shall provide opportunities for management and supervisory training for Sheriff’s Office supervisory staff in the subjects of career development as needed.

C. The Office shall utilize its resources, regional training programs, staff meetings and/or required continuing education articles from professional journals to accomplish management and supervisory training.

5. **Training Record Maintenance:**

A. The Training and Educational Services Bureau shall maintain accurate and updated records of members’ certifications and/or attendance at training programs, type of training, and available test scores (all recruit, in-service and specialized training).

B. The Recruit Training Unit shall maintain records for all recruit personnel to include the following at a minimum:

1. Course name and course content
2. Name of attendees
3. Performance of individual attendees and measurement used (test)

C. The Advanced Training Unit shall maintain records for certified deputies to include the following at a minimum:

1. Course name and course content
2. Name attendees
3. Performance of individual attendees and measurement used (test)

**NOTE:** Paper and electronic storage are acceptable methods of retaining Training Records and Documentation.

D. For all external training not offered by the Office, it shall be responsibility of personnel to provide the Training and Educational Services Bureau with a copy of the certificate of achievement/attendance as soon as possible following receipt from the training source. It should be noted that TESB shall maintain a list of training sources, which are Sheriff approved according to subject. In this way, the Sheriff’s Office training and knowledge base is as uniformed as possible.

E. The Unit Commander of each unit is responsible for disseminating all policies and training materials to deputies under her/his command as soon as they become available. The Chief Deputy shall conduct periodic audits of training records to ensure that deputies are current with training and certifications.
6. **Record Retention**

A. All records shall be stored on-site with the TESB. Record retention shall be guided by the Record Retention Schedule issued by the Sheriff. All training and certification records shall remain in the employee's training file until her/his retirement.
Philadelphia Sheriff's Office

DIRECTIVE: #34
SUBJECT: TRAUMATIC INCIDENTS
ISSUE DATE: 04-09-2020
REVISED DATE: 02-24-2021

I. PURPOSE:

A. This General Order applies to any department employee, sworn or civilian, who is involved in a traumatic incident. It is not intended to displace or contradict Critical Deputy Involved Critical Incident (DICl) investigative processes, but to facilitate the prompt access to assistance and return to work.

B. This Directive establishes standardized selection guidelines for the process used to fill assignment vacancies. The allocation of personnel to a specific assignment is designed to promote efficiency and to optimize departmental effectiveness while considering the needs, knowledge, skills, abilities, and preferences of the individual employees. Although not mutually exclusive, at times both objectives may not be simultaneously achievable.

II. DEFINITIONS:

A. Traumatic Incident: for the purposes of this section, includes shootings, accidents and other incidents that result in the serious bodily injury or death to any person.

B. Traumatic Incident Leave is a standalone Philadelphia Sheriff option to grant sick time as a paid reprieve from regular duties for up to three (3) workdays after being involved in a law enforcement related traumatic incident. Upon the approval of the Sheriff, or designee, the leave will commence on the employee’s first regularly scheduled shift after the traumatic incident.

C. The Traumatic Incident Coordinator (TIC) is an employee (the Sheriff’s Office, Chief of Staff) appointed by the Sheriff who serves as a point of contact during a traumatic incident.

D. The Peer Support Team is defined in the Wellness Unit Directive- #58.
E. The Wellness Unit is defined in the Wellness Unit Directive- #58.

F. Occupational injuries/illness is caused by exposure to factors associated with the scope of employment. Workers Compensation claims may be filed for physical or psychological occupational injuries.

III. TRAUMATIC INCIDENT LEAVE

A. Deputies who, in the scope of their duties as a law enforcement officer, cause the death of another person are required to take Traumatic Incident Leave.

B. If above III-A does not apply, employees, sworn or civilian, involved in a traumatic incident in the scope of their duties as an employee of the Sheriff’s Office may request to take Traumatic Incident Leave.

1. The division Deputy Chief has the discretion to verbally activate the policy and require employees impacted by a traumatic incident to take Traumatic Incident Leave.

C. The first workday after the traumatic incident will be defined as Day 1 of Traumatic Incident Leave and the employee will not report for duty.

D. The second and third workdays, will be defined as Day 2 and Day 3 of Traumatic Incident Leave, and the employee will be on administrative duties as directed by the Traumatic Incident Coordinator. The employee will report to the Deputy Chief, Training Division at 100 S. Broad Street-6th Floor, or other agreed upon location.

E. If the employee has a regularly scheduled day off, or pre-approved day off, the Traumatic Incident Leave will commence or resume on the employee’s first regularly scheduled shift after the incident.

F. If the employee is injured during the incident and must take occupational leave, the occupational leave day(s) will count as part of the Traumatic Incident Leave.

G. The employee will meet with the Traumatic Incident Coordinator and the Deputy Chief, Training Division at 100 S. Broad Street-6th Floor or at another agreed upon location on the employee’s first scheduled shift after the three (3) days of leave.

H. The employee will be available to meet with other Sheriff’s Office or Police Department officials as necessary, i.e., Detective Division, IAD, the Undersheriff, City Solicitor’s Office, Firearms Technicians/Range Instructors, etc. The Traumatic Incident Coordinator, Wellness Unit member or Peer Support Team member will be available to accompany or escort the deputy to these meetings, as requested.

IV. SUPERVISORY ROLES AND RESPONSIBILITIES

215
A. At the time a traumatic incident occurs, the first line supervisor should communicate with the Traumatic Incident Coordinator or designee upon his/her arrival on site.

B. The supervisor will be responsible for reviewing and approving time sheets for the period the employee is on Traumatic Incident Leave, in compliance with this directive.

C. If a supervisor has a concern about how an employee under his/her authority is dealing with the traumatic incident, they are encouraged to provide the employee the list of Available Resources for Assistance, i.e., Philadelphia Sheriff’s Office Wellness Unit, Employee Assistance, and to notify the employee’s chain of command.

V. ROLE OF THE TRAUMATIC INCIDENT COORDINATOR (TIC)

A. The TIC is an employee (Chief of Staff) appointed by the Sheriff. The Traumatic Incident Coordinator will be available at any shift on any day to provide options to the involved employee to facilitate the employee making informed decisions about their mental health. The TIC may designate the Commander of the Wellness Unit to fulfill this role at any time.

B. The TIC will provide the employee with the Available Resources for Assistance in memo format. The Traumatic Incident Coordinator is not authorized to accept medical information but may direct the employee to the Undersheriff or the HR Director for assistance in filing a Workers’ Compensation claim.

C. The employee is not required to disclose information to the Traumatic Incident Coordinator about the traumatic incident but may do so at his or her discretion.

1. The Office of the Sheriff will endeavor to maintain confidentiality but will be required to release information as required by law.

2. No information or details shared with the Traumatic Incident Coordinator will be disclosed to any party without the employee’s knowledge unless required by state or federal law.

VI. RETURN TO REGULAR DUTIES

A. Prior to the end of Day 3 of Traumatic Incident Leave, the employee will meet with the Traumatic Incident Coordinator and/or the Wellness Unit Commander to determine readiness to return to work and other available options.

B. The employee may return to his or her regular duty assignment, provided there are no medical restrictions.
C. In any incident, where a fall or any harsh physical the employee may submit a Workers’ Compensation Claim, by filing a First Report of Injury and sending that information to Human Resources. This may result in occupational leave or medical restrictions that limit the employee’s duties.

D. The employee may utilize personal leave in accordance with policies.

E. The employee may request a temporary reassignment to other duties that serve the Office of the Sheriff needs and best utilize the employee’s skills and experience. Temporary assignments are made by the Sheriff or designee. The Sheriff or Designee may place the employee in one of the positions available to officers on medically limited duty but will not create a new limited duty position.

F. The appropriate Deputy Chief, in consultation with the Traumatic Incident Coordinator or Wellness Unit Commander, may override the decision of the employee to return to full duty and recommend a temporary assignment, or encourage the employee to seek additional evaluation by an appropriate medical provider, if it is in the best interest of the employee and/or the Office of the Sheriff.

G. In the event a temporary reassignment is found, the Office of the Sheriff reserves the right to review the status of the employee and his/her temporary assignment every fourteen (14) workdays.

VII. CONFIDENTIALITY

A. It is expected that any person involved in the traumatic incident process maintain the highest standards of professional conduct, and respect the privacy of the involved employee by not sharing any information regarding the incident, or the persons involved, unless at the request of the Sheriff or designee, the City Solicitor’s Office, the court, or as required by state or federal law.

BY ORDER OF:

\[Signature\] 
SHERIFF DATE

217
III. PURPOSE:

A. Peer Support Team members are not counselors or therapists but are specially trained colleagues who volunteer their time to provide intervention and assistance to Office of the Sheriff employees involved in traumatic incidents and in times of personal and/or professional crisis. These team members shall not be additionally compensated by the Office of the Sheriff for the work done as peer support team members. All such work shall be done in addition to the employee’s regular duties, on a voluntary basis. The City of Philadelphia Employee Assistance Program (EAP) Manager will oversee the team.

B. Information provided to members of the Peer Support Team is not protected by legal privilege; however, communication between Peer Support Team members and employee is confidential through this Sheriff’s Office mandated policy and shall not be subject to any administrative investigation. The exceptions to confidentiality occur in cases where the law requires divulgence:

1. A danger to self or others,
2. Suspected child abuse,
3. Narcotics offenses,
4. Domestic violence,
5. Factual elderly abuse, or
6. Felonies and serious misdemeanors.

C. When employees are directed to seek assistance from the Peer Support Coordinator or EAP by the department, only the supervisor or command staff with the need to know may be informed of the employee’s compliance with the directive.
D. The Peer Support Team is supervised by the Chief of Staff, who serves as the Peer Support Coordinator, or Team Leader. The Deputy Chief-IAD shall:

1. Select from volunteers, the employees who shall make up the unit. Applicants must be sworn deputy’s or full-time Office of the Sheriff Department employees in good standing. An interview process will occur and the Coordinator, with the assistance of the EAP Manager, will recommend applicants that appear to be best suited for peer support. The Coordinator will forward the list of recommended applicants to the Chief Deputy for review. After review, the Chief Deputy will forward a final list of recommended applicants to the Sheriff for approval.

2. Maintain an accurate roster of the names, telephone numbers, duty assignments, and other information regarding availability of team members who may respond when needed. The Peer Support Coordinator shall provide this list to the on call IAD supervisor.

3. Design and provide any specialized training the department requires to perform peer support, stress management, or crisis intervention activities.

4. Upon request by the command staff, at the time a disciplinary action has been initiated, intervene on behalf of any deputy or full-time employee of this Office to determine if the root cause may be other than a disciplinary matter, and provide any needed assistance and/or referral as necessary.

IV. RECALL FOR PEER SUPPORT TEAM:

A. Incidents subject to recall include but are not limited to:

1. Officer involved in a shooting with serious injury or death.

2. Officer involved in a major vehicle accident involving serious bodily injury or death.

3. Any similar incident that might be viewed as a cause of serious psychological stress upon the officer or police employee.

B. The Peer Support Coordinator shall be contacted by an on-call IAD Supervisor when an Office of the Sheriff supervisor has requested the services of the Peer Support Team. The Chaplain shall be notified if requested by the employee.

C. Notification of a peer support team member shall be initiated by the Peer Support Coordinator through the on-call IAD Supervisor. On-duty members shall be given priority in selection due to the importance associated with rapid response; however,
deputies or employees may specifically request any peer support team member on the active list.

D. The team member may be allowed to accompany the employee through all phases of the investigation, if requested by the concerned employee and with the permission of the investigator. The peer member’s status is not official, and they shall take no part in the investigation. Under no circumstances shall the peer member do anything that might disrupt or interfere with the investigation. The Peer Support Coordinator shall be responsible for the supervision of the team member working with the concerned employee during the initial phases of their contact.

E. Peer Support Team members shall not be used for sworn duties when off duty and acting in their capacity as a peer support team member.

F. Peer Support Team members shall maintain confidentiality for all conversations they are a party to between the deputies and/or employees when performing confidential peer support duties or be subject to disciplinary action.

V. REASSIGNMENT OF PERSONNEL INVOLVED IN A MAJOR INCIDENT:

A. Deputies involved in shootings, accidents, or other major incidents which result in death or serious injury to any of the parties involved, may be temporarily reassigned to other duties by the Sheriff or designee.

B. This reassignment is not automatic and is subject to review and concurrence by the Sheriff or designee after the request is made by either the deputy involved, a division captain with concurrence of their Bureau Deputy Chief, or the Peer Support Coordinator.

C. The reassigned position shall be determined by the Sheriff or designee and shall conform, as closely as possible, to the employee’s normal tour of duty.

D. The duration of the temporary assignment shall be decided by the Sheriff or designee upon determination that the employee has had sufficient time to read and has successfully recovered.

E. During the period of readjustment, if so indicated or requested, the Peer Support Coordinator may meet with the deputy and/or refer the officer to an outside professional or agency for counseling. This referral shall in no way indicate Office of the Sheriff liability for subsequent treatment.
F. This procedure shall not affect the prerogative of the Sheriff to place an employee on detached duty or any other restricted status.

BY ORDER OF:

[Signature]

SHERIFF       DATE
Philadelphia Sheriff’s Office

DIRECTIVE: #36
SUBJECT: INFORMATION TECHNOLOGY: OPERATIONS POLICY
ISSUE DATE: 03-02-2020
REVISED DATE: 02-24-2021

I. PURPOSE:

A. This Directive outlines the information technology security and confidential data protection policies and procedures that provide the framework of The Philadelphia Sheriff’s Office (the Office) technology protection and deployment. This is designed to serve as a directive to the officers, staff, users, information technology practitioners, contractors and stakeholders for the use, protection, and professional disposal of confidential data.

B. To allow for best practices data protection with regards to the specific information of the Office, this directive specifically mandates:

1. All technology in use by the Office is governed by an operating system patch process that works to ensure the most up to date and correct patches consistent with the operating system have been applied.

2. All deployed workstations of the Office are required to have computer virus protection software installed and operational. This directive is designed to be an effective and efficient prevention of network virus outbreaks and network security attacks involving computers associated with the Office. The primary focus is to ensure that Office users are aware of and take responsibility for the proper use of the Office-provided and supported virus protection software. This policy is intended to ensure:

   a. The integrity, reliability, and good performance of Office computing resources.
   b. That users operate according to a minimum of safe computing practices.
   c. That the office licensed virus software is used for its intended purposes; and
   d. That appropriate measures are in place to reasonably assure that this policy is honored.
3. This directive is to ensure that digital storage devices which contain licensed software programs and/or Office data must be reliably erased and/or destroyed before the device is transferred out of the control of the Office of the Sheriff, or erased before being transferred from one department, division or individual to another. The Office is committed to compliance with federal, state, and local statutes associated with the protection of confidential information as well as ensuring compliance with software licensing agreements.

4. With the mass explosion of Smart Phones and Tablets, pervasive and continuous wireless connectivity is almost a given at the Office. Insecure wireless configuration can provide an easy open door for malicious threat actors.

II. POLICY FOR GENERAL TECHNOLOGY

A. It is the policy of this Office that the technology in use and deployed adhere to the following standards:

1. Security vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software which can disrupt normal Office operations in addition to placing Office data at risk. In order to effectively mitigate this risk, software "patches" are made available to remove a given security vulnerability. Given the number of computer workstations and servers that comprise the Office network, it is necessary to utilize a comprehensive patch management solution that can effectively distribute security patches automatically when they are made available. Patches may be automatically installed and, when necessary, the affected machine rebooted. Effective security is a team effort involving the participation and support of every Office employee and affiliate who is a user of the Office computer network.

   a. This policy applies to employees, contractors, consultants, temporaries, and other workers at the Office including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Office such as all electronic devices, servers, application software, computers, peripherals, routers, and switches.

   b. Many computer operating systems such as Microsoft Windows, Linux, Mac OS, and others include software application programs which may contain security flaws.

   c. Occasionally, one of those flaws permits a hacker to compromise a computer. A compromised computer threatens the integrity of the network and all computers connected to it. Almost all operating systems and many software applications have periodic security patches released by the vendor that need to be applied. Patches which are security related or critical in nature must be installed.
d. In the event that a critical or security patch cannot be centrally deployed by IT, it must be installed in a timely manner using the best resources available. In the case of non-Microsoft desktop operating systems where a centralized deployment is not available then installation should occur in a timely manner by a member of the IT Support team.

e. Failure to properly configure new workstations is a violation of this policy. Disabling, circumventing, or tampering with patch management protections and/or software constitutes a violation of policy.

2. Centrally provided virus protection software must be run on all Office computers and on all computers connected to The Office computer network. A management structure and supporting guidelines and procedures have been defined and will be utilized to implement the above policy and ensure compliance.

a. Virus protection is most effective if every computer on the Office network has anti-virus software installed and is actively monitoring network activities. The Office will 1) provide the setup for all computers; 2) update and monitor virus protection updates daily to be sure signature updates are current; 3) provide scanning of incoming email for virus and malware, including attachments.

3. Reasonable steps must be taken to ensure that all confidential data is rendered unrecoverable prior to reuse or disposal of the media on which it was stored. Data destruction must be done according to the guidelines in this standard. Any other destruction methods must be approved by the Sheriff or the Chief Deputy. Contractors must create and follow procedures to ensure that all devices and media are processed in accordance with these standards. Between the time that media containing confidential data is removed from service, and the time it is sanitized or destroyed, it must be safeguarded. Evaluate possible storage spaces with the same security used for locating production systems used with confidential data. Compliance with this standard does not obviate the need to comply with public records law. Before data destruction, IT must verify compliance with the Office through the Undersheriff and Court records disposition requirements.

4. The purpose of this policy is to secure and protect the information assets owned by the Office. The Office provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives.

a. This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to Office network and devices such as laptops, tablets, and cell/smart phones ("Devices"). Only those wireless infrastructure devices that meet the standards specified in this policy or are granted a documented exception by the Office CISO are approved for connectivity to the Office Devices.

b. All employees, contractors, consultants, temporary and other workers at the Office, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of the Office must adhere to this policy. This
policy applies to all wireless infrastructure Devices that connect to the Office Device or reside on an Office site that provide wireless connectivity to endpoint Devices including, but not limited to, laptops, desktops, smart/ cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

c. Wireless General Requirements

1) All wireless infrastructure devices that are used by Office Devices at a site and connect to a network, or provide access to Office information must:

   (i) Abide by the standards specified in these Wireless General Requirements.
   (ii) Be installed, supported, and maintained by an approved support team.
   (iii) Use Office approved authentication protocols and infrastructure.
   (iv) Use Office approved encryption protocols.
   (v) Use of a known SSID (Service-Set Identifier)
   (vi) Maintain a hardware address (MAC address) that can be registered and tracked and not interfere with wireless access deployments maintained by other support organizations.

d. Lab and Isolated Wireless Device Requirements

1) All lab wireless infrastructure devices that provide access to Office information must adhere to Wireless General Requirements above. Lab and isolated wireless devices that do not provide general network connectivity to the Office network must:

   (i) Be isolated from the office network (that is it must not provide any corporate connectivity) and comply with the Lab Security Policy.

   (ii) Not interfere with wireless access deployments maintained by other support organizations.

e. Home Wireless Device Requirements

1) Wireless infrastructure devices that provide direct access to the Office Devices, must conform to the Wireless General Requirements above.

2) Wireless infrastructure devices that fail to conform to the Wireless General Requirements above must be installed in a manner that prohibits direct access to the Office network.

3) Access to the Office corporate network through this device must use standard remote access authentication.
f. Public Wireless Device Requirements

1) Public Wireless Devices that are typically found in public spaces, do not fit the Wireless General Requirements above and may never be used to connect Office Devices.

III. PROCEDURE:

A. To enable this Directive, the technology used by the Office end-users and deployed by the Office CTO/CISO through the Office of Information Technology (OIT) must follow the following procedures:

1. The purpose of this procedure is to describe the process for automated software updates to Office computers. Referred in the industry as patch management, a well-planned and documented management update process will produce a fleet of stable and consistently configured desktop computers that are secure against known vulnerabilities to the computer operating system and application software. This document describes procedures used by the Office’s IT services to achieve these goals. This procedure document is intended for all Office Employees.

a. Patch Classification

1) The Office divides patches into three basic categories in patch policies: Microsoft Updates, Apple Updates, and Third-Party Updates.

b. Microsoft Updates

1) Microsoft Updates are sub-divided into Core Patches (security and critical updates) and Optional Patches (non-security updates). Only Microsoft security update rollups are tested by the NOC.

2) To delay Windows update rollups for Network Operations Center (NOC) testing and deployment, The Office installed tool set disables the Windows Automatic Update feature on patch-managed resources. As a result, Updates were installed displays NEVER, simply indicating updates were not installed through Windows Automatic Update.

c. Core Patches consists of:

1) Security updates: Primarily contain Microsoft Monthly Rollups, which are consolidated sets of security fixes released each month for Windows 10, 8.1 and 7 SP1 machines, as well as Windows Server 2016, 2012 R2, 2012, and 2008 R2. May also contain security updates to Windows versions not impacted by rollups, such as Windows 7, 8, and Vista.
2) Critical updates: Fixes for a specific problem that address a critical, non-security-related bug.

d. Optional Patches (Non-Security Updates): other non-security Microsoft updates and consist of the following:

e. Definition Updates (not recommended): fixes for a specific problem that address a non-critical, non-security-related bug. Includes Microsoft’s Preview patches for the next Tuesday patch release. These updates are not recommended and are more likely to break existing applications and cause issues for the Office.

1) Definition updates: Frequent software updates that contain additions to a product’s definition database, which is used to detect objects with specific attributes, such as malicious code, phishing websites, or junk mail.

2) Tools: Utilities or features that help complete a task or set of tasks.

3) Drivers (not recommended): Software that controls the input and output of a device.

4) Application Service Packs: A tested, cumulative set of all hot fixes, security updates, critical updates, and other updates. Service packs may contain fixes for problems found internally since the product's release or may contain customer-requested design changes or features.

f. Microsoft Security Patch Testing

1) All Microsoft Core Patches listed must be tested. Patch management can be a very time-consuming process for both the Office and IT Professionals. By delaying the installation of Microsoft’s monthly security patch rollup, the team is able to extensively test the different patches within the rollup on the Office’s behalf—helping you identify and remediate issues before they happen and provide a better overall patching experience to the Office.

2) Additionally, delaying the installation provides other software vendors with time to release updates that fix known issues, provides the Office a greater likelihood of avoiding additional problems.

3) The goal of this process is to minimize Office technology issues so that operations continue to run smoothly. With the defined patch testing process, the Office does not just get a patch management tool; The Office gets a complete team that enables the Office to receive a better patching experience.

g. Test and Manage Security Patch Rollups
1) Patching is an important service that is provided to the Office to help keep their software secure, up-to-date, and running efficiently. However, new patches often cause issues with existing applications which can create additional work for the IT team and result in lost productivity for the Office. To avoid these problems, it's important to thoroughly test new patches before deploying them.

2) To help the Office reduce the number of issues experienced when installing Microsoft’s monthly security patch rollup, Network Operation Center (NOC) technicians must conduct extensive testing to identify any errors and conflicts with a list of existing applications so that the Office can have a more efficient and comprehensive patching experience.

3) The following graphic provides an overview of the Windows security rollup patch testing process:

```

Patch Tuesday

i. Day 1: Patch Tuesday
   - Microsoft releases their monthly security patch rollup on Patch Tuesday, the second Tuesday of each month. At this time, the installation of this rollup must be delayed for two weeks in order to thoroughly test how the installation impacts common business applications.

ii. Day 11: Patch Testing Report Published
   - 11 days after Patch Tuesday, a report is published that lists any issues identified during testing, and (if applicable) provides steps to avoid or remediate the issue. This report also includes any previously blacklisted patches that will be included in the monthly rollup.

iii. Day 14: Patch Rollup Released
   - 14 days after the patch rollup is made available, it is marked as NOC Tested and made available for download and installation according to the existing patch policies software.
```
- These patches are not tested by the NOC are deployable through the tool set patch policies after the first patch assessment scan is released by Microsoft.

h. Apple Updates

1) Apple updates are available as needed by Apple and include updates for Apple applications and Mac. Apple updates are deployable through the toll set patch policies after the first patch assessment scan is released by Microsoft.

i. Third-Party Updates

1) The Third-Party Updates option allows the Office to patch specific third-party applications, such as Adobe Flash Player, Apple Safari, and Mozilla Firefox. Third-party patches are available to the Office 15 days after release by the vendor. Patches support minor version updates (i.e., version 2.1 to version 2.2). Major version update support is offered for selected applications.

2. The purchased anti-virus software program **SHALL** be able to:

1. Prevent all infections. When that is not possible, the anti-virus software program should create an outlet for notification and annotation of virus outbreaks for end-users to promote the prevention of future breaches.

2. Prevent the loss of information/data and software on Office-owned computers and minimize the cost of computing maintenance and network downtime by virus outbreaks.

3. Maintain updates of virus protection software and other important Office-supported software. Virus protection software that is not used cannot prevent infections.

4. Annually evaluate the number of virus outbreaks to determine whether this policy and the office-provided virus protection software are still valid and appropriate.

5. Provide and continue to support the best virus protection solution that The Office can support.

6. Require a minimum of end-user responsibilities for computer virus protection practices.

3. The destruction and sanitization of media in the Office **SHALL** follow these procedures:
1. Media and devices containing confidential data that will be stored or transported prior to destruction should be inventoried in case of loss before data is destroyed. Inventory documentation should include a unique identifier where appropriate (such as a hard disk model and serial number, an item or lot description, or description of data records).

2. Inventory documentation should be retained at least until the media or device is destroyed. If the media or device will be destroyed by an authorized contractor, obtain certification of destruction.

3. All electronic storage media should be sanitized when it is no longer necessary for Office use, provided that the sanitization does not conflict with any Office data retention policies.

4. All electronic storage media should be sanitized prior to sale, donation, or transfer of ownership. A transfer of ownership may include transitioning media to someone in your department with a different role, relinquishing media to another department, or replacing media as part of a lease agreement.

5. All Philadelphia Sheriff’s Office employees are responsible for the sanitization of non-reusable electronic media before disposal. Similar to shredding paper reports, CDs and other information storage items, non-rewritable media shall be professionally destroyed prior to disposal.

6. Pursuant to this directive, Divisional Deputy Chiefs are responsible for the prerequisite means of sanitation of all Office owned electronic devices and computer systems in their units prior to removal from the workplace. This responsibility may be delegated within the Office as deemed appropriate.

7. Any disposal of computer equipment, copiers, peripherals, and media storage devices must comply with all surplus disposal procedures as defined by the logistical services department and this directive.

8. The following table (Table. 1) lists minimum recommended methods of confidential data destruction for various devices and media types. Other methods may suffice for other data.
Table. 1  Minimum Destruction Methods for Media

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Minimum Data Destruction Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functioning hard disks that may be re-used</td>
<td>Minimum 3-pass overwrite, or utilization of ATA Secure Erase feature</td>
</tr>
<tr>
<td>Hard disks that are damaged or will not be re-used</td>
<td>Degauss</td>
</tr>
<tr>
<td>Tapes (video and data backup)</td>
<td>Degauss or 3-pass overwrite</td>
</tr>
<tr>
<td>Flash media-based devices (USBs aka thumb drives, memory cards)</td>
<td>Minimum 3-pass overwrite in a way that ensures all storage space is overwritten</td>
</tr>
<tr>
<td>CD, DVD, floppy disks</td>
<td>Cross-cut shredding</td>
</tr>
<tr>
<td>Devices such as PDAs, phones, digital audio/video players</td>
<td>Cell Phone Data Eraser, such as <a href="https://www.ontrack.com/products/data-erasure/mobile-erase/or">https://www.ontrack.com/products/data-erasure/mobile-erase/or</a> similar. Also see brand/model specific guidance.</td>
</tr>
<tr>
<td>Confidential data containing Media and devices</td>
<td>Incineration, pulverization, disintegration (These methods should be reserved for media and devices that once contained confidential data or are non-functional, obsolete, or have no other practical method of destruction.)</td>
</tr>
</tbody>
</table>

8. Vendors contracted for professional data disposal shall be certified by the National Association for Information Destruction (NAID). When in doubt about the proper procedures for device, contact the manufacturer AND the IT Director.

9. Wireless General Requirements Compliance Procedures

   a. The IT team will verify compliance to this policy through various methods, including but not limited to, periodic site inspections, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.
IV. **ENFORCEMENT**

A. Any person found to be in violation of this policy and procedure will be subject to appropriate disciplinary actions as defined by current Office of the Sheriff directives, city/county IT policy and/or collective bargaining agreements.
VI. PURPOSE:

A. It is the responsibility of each employee to engage in and promote workplace behaviors that create and maintain an environment of respect and that promote effective teamwork. Employees shall report behaviors of a harassing nature to a supervisor. Employees have a cause of action for a hostile work environment when:

1. The employee was subjected to unwelcome harassment based on a protected trait such as race, gender, religion, age, and disability.

2. The harassment affected a term, condition, or privilege of the employee's employment.

3. The employer knew or should have known of the harassment; and

4. The employer failed to take prompt remedial action.

B. Any supervisor or manager who learns of an allegation of hostile work environment has a duty to take prompt remedial action to protect the alleged victim and to investigate promptly and thoroughly all claims of harassment whether:

1. A complaint is made in writing or verbally.

2. The complainant wants an investigation or does not.

3. No actual complaint has been made; however, the supervisor has a constructive knowledge of the harassment.

C. Supervisory/Management Responsibilities:
a. Work Environment: Managers and supervisors are responsible to maintain a work environment that is free from harassment and discrimination, and therefore are responsible for the conduct of their subordinates and non-employees present in the workplace. Any manager or supervisor’s failure to affirmatively act to comply with this responsibility may result in discipline.

b. Duty to Report: Any supervisor or manager who receives a harassment/sexual harassment complaint or has reason to believe that harassment/sexual harassment is occurring shall report the complaint to the relevant HR Department Manager for processing in accordance with this policy. Failure to report any such complaint is grounds for disciplinary action.

c. Standard of Conduct: Supervisors will be held to a higher standard of conduct and will be the subject to a higher level of discipline when engaging in harassment/sexual harassment.

VII. HARASSMENT POLICY:

A. It is the policy of the Office of the Philadelphia Sheriff (the Office) that it is the responsibility of harassment in any form is strictly prohibited. All employees shall be provided a professional work environment representative of fair and courteous treatment that is free of any intimidation, hostility, or harassment.

B. Visuals

1. The Office of the Sheriff prohibits:

a. Displaying, publicizing, or possessing graphic materials that are in any way sexually revealing, sexually suggestive, sexually demeaning or pornographic in the work environment, such as pictures, screen savers, posters, cartoons, calendars, graffiti, objects, promotional materials, reading materials, websites, GIFs (graphics interchange formats), memes, social media or other materials;

b. Graphic content will be presumed to be sexually suggestive if it depicts a person who is nude or semi-nude and/or who is posed for the obvious purpose of displaying or drawing attention to private portions of the body, with exceptions considered in situations where nudity or sexually explicit language is necessary to convey a message important to public health and/or public safety;

c. Displaying signs or other materials purporting to segregate an employee by sex in any area of the workplace (other than restrooms and semi-private lockers/changing rooms).

C. Gender Identity/Sexual Orientation
1. The Office of the Sheriff prohibits all unwelcome conduct, or for purposes of this policy, unwelcome means unwanted. No employee should ever assume any such conduct is welcome by others.

2. The Office of the Sheriff also prohibits conduct based on one’s sexual orientation, or gender identity. Prohibited conduct includes but is not limited to:

   a. Stereotyping of offensive comments that denigrate or insult someone because of sex, sexual orientation, or gender identity.

   b. Mis-gendering a person.

   c. Intentionally or consistently outing a person.

   d. Gossip or questions about someone’s sex, sexual experience, sexual orientation, gender identity, or anatomy, such as genitals.

   e. Intrusive questions regarding a person’s family formation or structure in terms of the gender of the spouse, person(s) they are cohabitating with, or romantic/sexual partner(s).

   f. Ostracizing someone or otherwise making it known to someone that they are not welcomed in the workplace because of their sex, sexual orientation, or gender identity.

D. Retaliation

1. It is unlawful to take adverse action against someone who files a complaint of harassment or discrimination, or who cooperates in the investigation of such a complaint.

2. Retaliation is a violation of the City and Office of the Sheriff policies, and employees who engage in retaliatory conduct are subject to appropriate discipline up to and including discharge and may incur legal liability. Examples of retaliation may include but are not limited to the following:

   a. Arbitrary discipline, unwanted change of work assignments, providing inaccurate work information, or failing to cooperate or discuss work-related matters with any employee because that employee complained about, has been a witness to, or resisted harassment, discrimination, or retaliation; and

   b. Intentionally pressuring, falsely denying, lying about, or covering up or attempting to cover up conduct such as described in any item above.
c. Intentionally ostracizing, excluding, or alluding to an employee, rather than exercising direct contact with the complaining employee when such contact would be otherwise direct absent the existence of any complaint.

VIII. SEXUAL HARASSMENT POLICY

A. This policy specifically includes the prohibition of sexual harassment in any form; establishing the goal of eliminating the incidences of sexual harassment by educating all personnel about improper conduct in the workplace and providing a professional work environment representative of fair and courteous treatment that is free of any intimidation, hostility, or harassment, and defining sexual harassment in comprehensive yet simple terms.

B. Sexual harassment of any degree or form in the workplace negatively affects morale, motivation, and job performance, and significantly damages the prospect of a harmonious working environment. Employees shall not engage in activities or conduct that may be perceived to be sexual harassment and sexual harassment of any form shall be considered serious misconduct.

C. Sexual harassment definitions: Although it is impossible to completely explain all prohibited behavior, the following represents a general explanation of what constitutes sexual harassment, all of which is prohibited in the workplace. The definitions listed below are in accordance with the guidelines adopted by the Equal Employment Opportunity Commission.

1. Unwelcome sexual advances, requests for sexual favors, and other verbal (slurs, jokes, allusions) or physical conduct of a sexual nature constitute sexual harassment when:

1. Submission to such conduct is made either explicitly or implicitly a term or condition of employment, or

2. Submission to or rejection of such conduct by an employee is used as the basis for employment decisions affecting the individual, or

3. Such conduct has the purpose or effect of interfering with an employee’s work performance or creating an intimidating, hostile, or offensive working environment, or

4. A person alleges conduct which a reasonable person would consider sufficiently severe or pervasive to alter the conditions of employment and create an abusive working environment.

5. Actions are consistent with section II, D-2c.
2. Sexual Favoritism occurs when employment opportunities or benefits are granted because of an individual’s submission to sexual advances or requests for sexual favors.

D. Specific prohibited behaviors include any unwelcome sexually motivated physical contacts, sexually derogatory statements, and verbal sexual advances. Work-related incidents which are sexual in nature or connotation and which an employee finds objectionable are prohibited. The following types of conduct are examples of sexual harassment and are prohibited. These examples do not represent all the ways in which sexual harassment may occur and are not intended to limit the definition of sexual harassment.

1. Examples of sexual harassment include but are not limited to:
   
a. Suggestive or obscene letters, notes, emails, texts, blog submissions, posts, and invitations.
   b. Verbal examples include sexually suggestive remarks, derogatory comments, slurs, jokes, and epithets.
   c. Visual examples include leering, gestures, or tangible or digital displays of sexually suggestive objects or pictures, cartoons, or posters.
   d. Physical examples include deliberate and unsolicited single touching of a sexual nature. Deliberate and unsolicited repeated touching of any kind includes touching, patting, pinching, the repeated brushing against another person’s body, or that is otherwise unwelcome.
   e. Threats that an employee will be adversely affected if sexual demands are rejected. Such threats include, but are not limited to, lower evaluations, denial of promotions, punitive transfers, terminations, and altered or increased work assignments.
   f. Explicit or implicit promises of career advancement or preferential treatment in return for sexual favors. Included, but not limited to, hiring, promotion, training opportunities, acceptance of a lower standard of performance, providing higher performance evaluations, and lax timekeeping. Denial of an employment opportunity or benefit to an individual because of refusal to submit to sexual advances. The provision of an employment opportunity or benefit to an employee because of submission to sexual advances when a similar opportunity or benefit is not granted to similarly qualified persons with whom the harasser is not sexually involved.
   g. Any number of unwelcomed contact or requests for dates or invitations to non-work-related events.

IX. PROCEDURE:

A. Determinants of Investigative Responsibility:

1. If the complainant is a sworn employee, the primary investigative responsibility rests with the City of Philadelphia Office of Employee Relations. The Office of
the Sheriff-Internal Affairs Division will be an investigative repository for the complaint, conduct its own simultaneous investigation or in conjunction with the Office of Employee Relations (ERU) and communicate any/all recommendations made by the Office of Employee Relations for education-based discipline, retraining, and /or disciplinary action.

2. If the complainant is a civilian employee, the Undersheriff (or Chief Deputy) will follow procedures in IV, A1.

3. When an investigation is enacted in all instances of Sexual Harassment, ERU will be notified by the Undersheriff, HR Director, or IAD-Deputy Chief.

B. Management Responsibilities: Prevention is recognized as the most effective means for the elimination of sexual harassment. Therefore, all supervisory personnel shall:

A. Act promptly and affirmatively when they observe behavior that violates this regulation, and/or when they receive complaints of sexual harassment.

B. Ensure sexual harassment does not occur and that a hostile atmosphere does not exist for any employee.

C. Personally, express strong disapproval for all forms of sexual harassment.

D. Enforce and ensure compliance with the sexual harassment policy.

E. Inform employees of the right to raise and the procedures for raising issues or filing complaints of sexual harassment with this department or other appropriate agencies.

F. Properly document and forward to Internal Affairs and the Human Resources Department, with a copy to the Female Employees’ Coordinator (if applicable), any reported incidents or complaints of sexual harassment.

G. Take immediate and appropriate action to preclude further aggravation of any incidents or complaints of sexual harassment.

H. Ensure all complaints of sexual harassment are dealt with in strict confidentiality to preclude retaliation or further harassment toward any involved employee. Any form of retaliation directed toward any employee who has filed a sexual harassment complaint will be dealt with swiftly and severely.

I. Develop methods to sensitize all employees within individual commands and supervisory areas of responsibility.
B. **Female Employees’ Coordinators:** A sworn member of command (captain or above) and civilian female member of the HR Department (Director or Deputy HR Director) and shall be assigned as Female Employee’s Coordinators as directed by the Philadelphia Sheriff or her/his designee. The Female Employee Coordinators shall:

1. Develop and participate in training programs on the Office of the Sheriff sexual harassment policy.
2. Assist in familiarizing all command and supervisory personnel with their responsibilities regarding sexual harassment.
3. Present mandatory sexual harassment policy training and orientation to all newly promoted supervisors.
4. Present sexual harassment policy training in conjunction with the Training Deputy Chief to all deputy sheriff trainee classes and to all newly hired civilian employees within one month of orientation process and before the new employee (sworn or civilian) assumes an active employment role outside of training.
5. Assist the ERU, Internal Affairs, and HR Director as needed with investigations into complaints or reported incidents of sexual harassment.
6. Shall review the final ERU’s Investigative Finding Report with Internal Affairs on all sexual harassment complaints.
7. Keep the Sheriff informed about documented or perceived incidents or complaints of sexual harassment.
8. Provide a written report to the Sheriff, as necessary.

C. The Female Employees Coordinators shall also be responsible for:

a. Coordinating activities and solutions to matters and concerns unique to female personnel.

b. Representing the department with agencies and/or organizations of interest to female personnel.

c. Assisting in recruitment or in developing recruitment activities for female deputies.

D. Chief of Staff: shall ensure that each Office of the Sheriff secured facility prominently displays copies of this directive AND the City of Philadelphia’s Sexual Harassment Prevention Policy as revised and disseminated 08/30/2019 (including all attachments).
E. Any complaint alleging harassment (of any type): shall be construed as being a claim against the Office of the Sheriff. Each complaint, unless determined by the Undersheriff/legal counsel post-ERU investigation to be facially invalid.

1. Complaints may be filed with the ERU, Female Employees’ Coordinator, their immediate supervisor, any other employee of supervisory rank, Internal Affairs, or the Human Resources Department.

2. Complaints may be made by telephone, email, memorandum, or in person.

F. Employees who desire to meet with the Female Employees Coordinator to discuss any concerns of sexual harassment may do so on duty.

1. Employees are under no obligation to report incidents of sexual harassment to their immediate supervisor prior to or subsequent to filing a complaint.

2. Any employee receiving written or verbal information of incidents involving sexual harassment shall properly document the information by the next workday and immediately forward the original complaint or report of the incident to Internal Affairs with a copy directed to the Female Employees’ Coordinator.

3. All complaints of sexual harassment filed with The Female Employee’s Coordinator or IAD shall be investigated and shall remain confidential, unless divulging the contents of the complaint must occur to promote the investigation of the complaint or will subject an employee to further harassment.

E. In all cases investigated of harassment (of any kind), the IAD-Deputy Chief or HR Director shall submit the final investigative report to the Female Employees’ Coordinator, Undersheriff, Chief Deputy, and Sheriff for review.

F. General Responsibilities of All Personnel

1. Individual preference may lead some employees who experience sexually harassing conduct to seek to resolve the problem by dealing directly with the offending individual. Employees are expressly not required to deal directly with an offending individual in seeking resolution of a complaint of sexual harassment.

2. Any employee feeling uncomfortable or having difficulty with a situation may obtain assistance from:

   a. The Female Employees’ Coordinator.
   b. Any Office of the Sheriff supervisor.
   c. The Office of the Sheriff-Human Resources Department.
   d. The City of Philadelphia City Controller’s Office
   e. The City of Philadelphia Employee Labor Relations Unit (ELRU)
f. Filing an online complaint from located at: https://
    beta.phila.gov/services/working-jobs/file-a-sexual-harassment-complaint/

    (City of Philadelphia’s Sexual Harassment Prevention Policy, 2018)

3. When faced with harassment of any type by a co-worker, you should:

   a. Give immediate and verbal notice to your harasser to stop.

   b. If harassment continues, go to a supervisor, any supervisor, the designated
      Female Employee’s Coordinator, or HR Director to make a complaint.

   c. When making the complaint, you must provide facts concerning the offensive
      behavior(s). These facts should answer the following:

         1) WHO committed the offensive behavior?
         2) WHAT was the specific behavior?
         3) WHEN and where did the incident(s) occur?
         4) WERE there any witnesses?
         5) DID the incident occur more than once?

4. Know that this directive legislates that any complaint made shall always remain
   confidential between the reporting party and the investigators (IV.F.3b). Any
   breach of confidentiality will be considered a violation of this policy and the
   offender(s) will be appropriately sanctioned.

5. Feel confident that any supervisor or Human Resources employee who fails to
   provide support thoroughly and fairly to the investigative process in complaints of
   any type of harassment will face disciplinary action and could face personal
   liability in the event of future litigation.

6. If the problem is still unresolved, you are counseled to maintain documentation
   and exhaust all avenues in-house, including, but not limited to union
   representatives, and to notify the next levels in the chain of command.

7. If the problem persists you are encouraged to exhaust all remedies, including
   proactively seeking outside assistance, such as the City of Philadelphia Office of
   Employee Relations, the Equal Employment Opportunity Commission [EEOC]
   and any Legal Remedies provided by Title 7 of the Civil Rights Act.

8. Reprisal or retaliation is strictly forbidden. This includes direct retaliation or
   reprisal or the encouragement of others to engage in retaliation or reprisal against
   any person who:
a. Opposes any conduct prohibited by this order, or

b. Complies or encourages others to comply with any provision of this order, or

c. Files a complaint concerning any violation of this order, or

d. Testifies, assists, or participates in any investigation or hearing resulting from a complaint under this order, or

e. Exercises or attempts to exercise any right conferred under this order.

9. Any employee of the city found to have engaged in sexual harassment; knowingly condoned, encouraged, or perpetuated an act or acts of sexual harassment; or found to have in some way participated in retaliation or reprisal, shall be subject to disciplinary action, including but not limited to suspension, loss of pay increment, demotion, and dismissal.

10. Where any employee of the city who claims to be the recipient of sexually harassing behavior and the investigation into the claim reveals the allegations were contrived, and therefore maliciously alleged, the employee shall be subject to severe disciplinary action up to and including termination.

11. Anonymous complaints will be investigated but may not lead to discipline for the offender if the complaint cannot be substantiated.

X. DISCIPLINARY ACTION

A. After a harassment/sexual harassment complaint has been investigated and the allegation substantiated, the following disciplinary actions shall be the guideline for Office of the Sheriff internal recommendations:

a. First offense: Written warning and mandatory counseling.

1. Discipline may rise to a maximum suspension of 10-days without pay depending upon severity of the offense; if offender is a supervisor; punishment may elevate to a maximum of 15-days without pay.

   NOTE: “Criminal Violation” does not mean a conviction is necessary to terminate the employee.

b. Second offense:
1. Discipline: A maximum suspension of 20-days without pay. If the offender is a supervisor, the punishment entails a demotion, and may also elevate to a maximum of 30-days without pay, depending upon the severity of the offense.

2. If the alleged offense is a criminal violation-termination.

NOTE: "Criminal Violation" does not mean a criminal conviction is necessary to terminate the employee.

c. Third offense: mandatory termination

XI. DUTY TO COOPERATE WITH INVESTIGATIONS

1. All employees and officials, including managers and supervisors, must cooperate with an investigation. Failure to cooperate may subject an employee to discipline, up to and including termination.

XII. FALSE CLAIMS

A. Any individual who levels a false claim of harassment or sexual harassment against another which results in disciplinary action against the falsely accused will be terminated from employment in this Department.

XIII. DUTY TO UNDERSTAND AND ADHERE TO CITY OF PHILADELPHIA SEXUAL HARASSMENT PREVENTION POLICY

1. It is the duty of all employees to understand and abide by the City of Philadelphia Sexual Harassment Prevention Policy (Aug. 30, 2019) attached to this directive.

BY ORDER OF:

[Signature]
SHERIFF
DATE

243
VIII. POLICY:

A. It is a tested law enforcement best practice in communication during a crisis to disseminate information as quickly and as accurately as possible to members of the public we are sworn to protect. In doing so, the Office of the Sheriff will convey verified, factual, information that avoids speculation or theory until an adequate assessment of the crisis can be made, and the response vetted. Crises that may involve rapidly expanding incidents, like an active shooter, a terrorist attack, cyber-attack, or any other imaginable or unimaginable emergency, can jeopardize adherence to even the best laid plans. Crisis scenarios are usually suddenly and unexpectedly, but while it is difficult to plan for something unpredictable, there are numerous planning steps that can be undertaken to preparation for times of crises.

B. When an emergency occurs, the need to communicate is immediate. If Office operations are disrupted, customers will want to know how they will be impacted. Regulators may need to be notified and fellow local government officials will want to know what is going on in their community. Employees and their families will be concerned and want information. Neighbors living near the facility may need information- especially if they are threatened by the incident. All of these “audiences” will want information before the Office has a chance to begin communicating.

C. An important component of the preparedness program is the crisis communications plan. The Office must be able to respond promptly, accurately, and confidently during an emergency in the hours and days that follow. Many different audiences must be reached with information specific to their interests and needs. The image of the Office can be positively or negatively impacted by public perceptions of the handling of the incident.

D. This directive provides direction for developing a crisis communications plan, while understanding potential audiences is key as each audience wants to know: “How does
it affect me?” Guidance for scripting messages that are specific to the interests of the audience is another element of the plan. The Contact and Information Center tab explains how to use existing resources to gather and disseminate information during and following an incident.

E. Law enforcement crisis communication plans should also cover scandals or incidents that could damage the reputation of the Office of the Sheriff. These may include things such as cases of employee misconduct, controversial use of force, or mishandled investigations.

F. In any case, a good crisis communication plan can help the Office of the Sheriff maintain public trust, protect its reputation, and quickly correct misinformation.

IX. **PRE-CRISIS ROLES:**

A. We start with a crisis communications team. The Executive Command leaders are going to be the ones held accountable in the public eye, so they need to be part of it. But when a crisis occurs, they may be consumed with other aspects of management, so the communications team will execute the plan and track the details. The Management Center has a useful framework for organizing project called MOCHA.

B. **MOCHA:**

1. **Manager:** Assigns responsibility and holds owner accountable. Makes suggestions, asks hard questions, reviews progress, serves as a resource, and intervenes if the work is off-track.

2. **Owner:** Has overall responsibility for the success or failure of the project. Ensures that all the work gets done (directly or with helpers) and that others are involved appropriately. There should only be one owner.

3. **Consultant:** Should be asked for input or to bring into the project needed resources or information.

4. **Helper:** Assists with or does some of the work.

5. **Approver:** Signs off on decisions before they’re final. May be the manager, though it might also be the executive director, external partner, or board chair.

C. **Executive Team Role**

1. Philadelphia Sheriff (Approver) will be the final approver.
2. Chief Deputy (Manager) will be the primary spokesperson and hold the owner accountable.

3. Communications Director (Approver/Consultant) will help with strategy and external relationships. Responsible for signing off on all decisions.

4. Public Information Officer (PIO) (Owner), will manage the communications, set strategy, collect all known information, assess the facts, assign tasks, approve outgoing messages and timing, and update leadership team.

5. Undersheriff, general counsel (Consultant) will help with legal issues and ensure that the communications taken into account our liability and sync with our legal strategies.

6. IT Director, cyber security specialist (Consultant) will help with technology and ensure that the communications sync with our other cyber crisis plans.

7. Chief of Staff and Unit heads, Staff (Helpers), will provide specialized knowledge and help disseminate information internally.

D. Meetings

1. The Chief of Staff will ensure the group meets quarterly. The purpose of the meetings is to simulate crisis scenarios and to ensure that team members are familiar and comfortable with the plan and their associated roles.

2. When the crisis hits, the crisis communications team will meet in the 5th floor conference room. If the room is inaccessible, the team will meet in the basement food court of the Bellevue building on the southwest corner of Broad and Walnut. If that is impossible, the group will meet via conference call.

Meeting Location

5th floor conference room >> Bellevue food court >> Secure conference line

E. Public materials

1. In a crisis, we’ll rely heavily on approved text and existing materials to make sure our identity is known, and our messages are consistent. Before the crisis, we need to carefully compose, edit, and review our materials with potential crises in mind.
2. It is critical to direct our messages in formats used to garner information regarding the Office of the Sheriff:

   a. The Office of the Sheriff website (Splash Pages, About Us, and Home Page).
   c. Sheriff’s Office Facebook Page.
   d. Sheriff’s Twitter.

3. The PSO Audience: This is a “living” contact list that is to be routinely reviewed and updated by the PIO and Chief of Staff. This list shall include constituents, internal and external stakeholders, and all persons reliant upon the services provided by the Office of the Sheriff.

   When drafting and approving messages, we will consider the following audiences:

   a. The sworn deputies and civilian employees of the Office.
   b. The voters and residents of Philadelphia, to whom we are accountable.
   c. The public-at-large.
   d. Other city officials and their staffs, especially the Mayor’s Office, and the Budget Office.
   e. The national law enforcement community; and
   f. Reporters, producers, and editors who will mediate (or potentially pervert) our messages to the other audiences.

4. PSO messages pass through different mediums to reach our audiences. This list shall be routinely reviewed and updated by the Chief of Staff. Among the channels we use are:

   a. Mainstream press, including TV, daily newspapers, news radio.
   b. Niche press, including community papers, ethnic and non-English papers, community radio, podcasts.
   c. Spanish-language radio, websites.
   d. Social media.
   e. Sheriff's website.
   f. Print and limited televised advertisements.

5. There is no substitute for efficient and effective management of all Office of the Sheriff operations. As the systems used by this department merge, several basic pieces of information will be crucial to have in a crisis, including:

   a. An accurate and updated contact roster inclusive of all employees.
b. Standardized Philadelphia Sheriff’s Office emails, phones, voicemail, and knowledge of how to retrieve messages remotely.
c. Remote access to our external contacts i.e., Outlook lite, encrypted phone access, cloud-based contacts, etc.

X. **CRISIS ROLES:**

A. Information gathering: The results or information gleaned in the first few minutes of any event. All crises are different, and will inspire different questions, but we will anticipate and prepare for the information gathering process by considering the following:

1. How are we likely to learn about a crisis? Internal sources? External sources? Social media? The news media?

2. How do we obtain more information about the crisis? Who leads the investigation or assigns investigators?

3. With whom do we share information with in the first minutes after learning about a crisis? Consideration must be given to both internal and external people stakeholders as well as affected public officials.

4. Be ready to respond quickly, even though we will likely not be certain of all the facts. It’s important to remember that the longer we’re silent, the more space there is for others to fill in their points of view, criticisms, or speculation. Even our friends might say something that hurts us despite their good intentions. Once we get our fact-based perspective out, media will have to reproduce it somehow in every story they do.

5. Our initial response should achieve four things:

   a. Position us as a source of facts and reliable information.
   b. Present facts from our point of view.
   c. Show our concern about the event and for those affected.
   d. Memorialize our statements in full. Utilizing YouTube, Facebook Live, Zoom, Skype, or other reviewable and accessible live streaming medium. This makes it difficult for others to pervert the message when you are providing the unedited message to everyone online.

B. **Silence = Circus:** What we absolutely cannot do is go silent. Silence will not stop the information flow; it conversely makes media fill the space with potentially inaccurate information. Detractors or people with destructive agendas from inside or outside of the organization will provide their versions of events, be critical, and appear factual. If we allow others to fill the information gap, it is a virtual guarantee that our side of
the story will be lost because we have lost control of the story itself; facts we know to be true are replaced with rumors and theories readily offered by others.

IV. **AFTER THE CRISIS:**

A. Step 1: Meeting

1. The first thing to do is conduct a Crisis Communications team meeting to take stock of the available facts and the gravity of the crisis, especially the worst-case scenario.

2. Meeting in person is important because it facilitates teamwork and expedites completion of tasks. The first meeting should produce a "hold" statement.

3. It should take place within 30-60 minutes after we learn about the crisis.

4. The meeting should include personnel with knowledge – preferably first-hand knowledge – of what transpired.

5. Review relevant approved language. Our approved language will come from our website and past press releases.

6. The best place to meet is 100 S. Broad Street, the Land Title Building-5th floor conference room. The backup location is the food court in the basement of the Bellevue. If neither location is possible, we will meet by conference call.

7. Talk about how we will avoid these common mistakes:

   a. **Covering things up.** We’ll get caught. Our audiences will forgive a mistake faster, but they will not forgive a cover-up.

   b. **Denying warning signs or ignoring internal issues.** If employees are whispering about problems, they are going to need to be addressed. Assess and address these issues: “Do it right. Do it right now”. This is more a management best practice thing than a messaging tenet.

   c. **Having an outsider speak for the organization, e.g., a lawyer or PR firm.** For a grieving family or a person on criminal trial, these are acceptable or necessary spokespeople, but for most everyone else, it is a bad look and fails to assign the proper weight to Office leadership.

   d. **Giving in to speculation.** Don’t share unconfirmed information. Stay factual. Don’t be dramatic. Confirm all facts before you say or repeat them.

   e. Absolutely avoid saying, "no comment" (which is what guilty people in movies say) or "I don’t know." We can say with absolute certainty that we’re looking into it, studying it, and investigating it. We can say “I’ll get you an answer,” or “I’ll find out for you.”
B. Step 2: Create a Hold Statement

1. Create a “hold statement” within one to two hours. In order to generate this, we can start with a journalistic approach by answering the “who-what-where-when-how” questions, and then think about what questions people are likely to ask or want to know. At a minimum, the hold statement must do the following:

   a. State facts. “Here’s what we know…”
   b. Give some sort of action plan, even if it’s just to conduct an investigation to get the facts. “We are collecting more information as we speak…”
   c. Provided a realistic timeline for updates; when will the facts be addressed, even if it’s very vague. “We will provide more details within the hour or as things develop…”

2. We have to be careful to distinguish facts from speculation, and only engage in verified facts. Information presented as fact can, and will likely, change. Theories and rumors will abound. In order to be considered a source of facts, we must recognize unverified information and avoid repeating it or entertaining speculation.

3. Hopefully, we’ll have time and enough verified facts to develop a more complete hold statement. It may make sense to do a second statement or an update with more details, or a more complete picture of the situation from our point of view. A more developed hold statement will:

   a. Be fact-based, not emotional, or promotional.
   b. Confirm pertinent known facts.
   c. Very briefly state our chief concerns.
   d. Be short and simple. We won’t yet have all the facts.
   e. Avoid speculation, even where things might make us look good, because it can come back to bite us later.
   f. Include an action plan.
   g. Set a timeline to share more information, even if the timeline is vague, like “later this week” or “in the coming days.”
   h. Express empathy for the affected audience; acknowledge feelings. A quote from Maya Angelou comes up again and again in the literature on crisis communications: “At the end of the day, people won’t remember what you said or did, they will remember how you made them feel.”

4. Here is more strategy for the hold statement:

   a. Devote additional attention to the tone and how it will be interpreted by the different audiences.
b. Choose the media through which we want to disseminate it. For example, if the crisis is happening on Twitter, consider put the statement on Twitter.

C. Step 3: Investigate the Occurrence

1. This is the point where we will consider hiring an outside firm that specializes in crisis communications. Every investigation will be different. The investigation itself may be out of the communications team’s hands, but its results and findings are important to how we frame the event. It’s important that communications are looped into the process. Some things to look for include:

   a. What was the problem that led to the event?
   b. Who’s responsible and who’s accountable? They may not be the same.
   c. What principle or value was violated? Does everybody agree? Does everybody agree that a mistake was made?
   d. How will we make sure it doesn’t happen again?

D. Step 4: Create a reactive statement

1. After more information has been gathered, we’ve sorted out different strategies, and prepared for the worst, we create a “reactive statement” and face our audience. When preparing the reactive statement:

   a. Keep in mind the same principles we used in the hold statement. Stick to facts; give a plan with a timeline. Make sure that among our audiences, we’re considering those who are or may have been affected.
   b. Brainstorm worst-case scenarios. What are the toughest questions we can imagine getting from the different audiences? Write out answers that address each with facts and empathy.
   c. Rehearse answers.
   d. Craft a brief opener to set the tone and clarify our position.
   e. Continue with a fact-based tone and narrative that addresses the major questions (not the worst-case scenario question, but the most likely things people and reporters will want to know).
   f. Apologize if necessary. It’s important to get this right and make sure it’s genuine. If it’s not, people will know. Consider not apologizing. When preparing an apology:

      i. Consider these three Rs: Remorse, responsibility, repair.
      ii. You can’t fake remorse. Don’t apologize just because the audience is mad; does it because you know you messed up. Definitely don’t say “I’m sorry people are upset,” or “I’m sorry if anyone was offended.”
iii. Accept responsibility. But make sure we’ve consulted the legal team first. We might not want to take responsibility.
iv. It’s possible to express sympathy without accepting responsibility, e.g., “I’m sorry that people were injured and that our vehicle was involved.” Be careful with this kind of apology.
v. Describe what we did that was wrong and say that it was wrong.
vi. Describe how we’re going to make things right.

E. Step 5: Review the crisis response

1. It’s always important to take a critical look at the moves we made, how they worked and what didn’t work as well as we’d wanted. This is also the time to examine our expectations and predictions along the line. We’ll ask what surprised us and how we could have prepared better for those events. Did we make assumptions we wish we hadn’t made? When constructing the review:

   a. Track the timeline. When did we first learn about the crisis? What was our response time? When did our messages go out?
   b. How did we learn about it? Did we go about getting more information in the best way possible?
   c. Gather our public messages and materials. Including anything that got out unintentionally (from us).
   d. How did the public respond to the event and to our messages? How did our response play in the media and the public?
   e. What happened that we weren’t expecting? What didn’t happen that we thought would happen?
   f. Did we get bogged down in groupthink? As we prepare for things, are we missing creativity or unorthodox ideas?
   g. Consider having a team that wasn’t closely associated with the crisis response review our response and what we released.
   h. Assess the outcome in the context of our overall performance measures. Did the crisis affect them? How did it affect us overall? Assess the messages for consistency both in tone and content. How did our policies change because of the crisis?

IV. CLOSING:

A. At this point, it may be best to put the crisis behind us and move on. Engaging further or adding comments could serve to unnecessarily prolong the story and taint what we do afterwards. However, the story may well continue to unfold. We may still be taking steps to address it. There may be good news to share along the way — or bad news to mitigate. There may also be some unaddressed loose strings remaining that impede our attempts to move past the crisis.

B. Consider creating a final statement, a post-crisis response (or a critical action review) to wrap things up and help our audiences accept the new post-crisis reality. Think
about what we’ve learned from the event and consider talking about some of those lessons. A good final statement could:

1. Say how the crisis has shaped the new reality.
   a. Answer any unanswered questions.
   b. Speak about it in the context of the new way of doing business.
   c. Did we learn anything from this?

2. Identify and thank heroes and advocates who helped bring us through and show gratitude.

C. Consider where to publish the statement, whether it be on the website, on social media, in a news release to the mainstream press.

D. Also consider NOT publishing or conducting a wrap-up statement. Maybe the crisis abated quickly, and we would only add momentum to something that doesn’t warrant momentum.

E. A crisis is not something that anyone wants or enjoys dealing with, but crises are inevitable parts of law enforcement and govern how we do business. We may not know what crises we might face, but we can be sure that we will absolutely face one (or multiple) eventually, and the best way to handle it is to prepare.

F. The crisis communications team quarterly meeting will review incidents that occurred over the past quarter and shall discuss and engage in role play on possible scenarios, crises that other organizations are facing, and even crises we’ve managed to avoid. The goals of these meetings are to learn before we make mistakes and to promote fluency with our plan and our team. A well-managed crisis exercise can strengthen an organization, and present new opportunities to grow, critique, and develop.

1. The Chief of Staff and PIO shall schedule (at minimum) quarterly practice scenarios to practice and refine the Office of the Sheriff potential response to incidents that may affect this Office or residents in the City/County of Philadelphia.
2. Civil Service Rank Supervisors shall receive the scenario-based training as professional development at least once bi-annually.
3. This training will be documented as Public Relations Training and logged by the Deputy Chief, Training Division.

BY ORDER OF:

[Signature]
SHERIFF DATE
DIRECTIVE: #39
SUBJECT: ROLL CALL AND INSPECTIONS
ISSUE DATE: 02-05-2020
REVISED DATE: 02-24-2021

A. POLICY:

A. It is the policy of the Office of the Sheriff that Uniform Services Division supervisors conduct formal roll calls at the start of each shift. The purpose of the roll call is to promote “Esprit de Corps” among the deputies, to ensure that each employee is ready and present for their shift, properly equipped, and remains informed of the latest information or intelligence available to all members of the Department.

1. All Uniform Services Divisions/Units at all facilities will adopt the roll call procedure described herein for each shift, every day.

2. Uniform Services Division Captains shall be responsible for exercising command and control of their assigned facility on a twenty-four (24) hour basis and shall therefore attend at minimum one (1) roll call per workday.

3. All roll calls will be conducted by the platoon lieutenant and a squad sergeant. In the lieutenant’s absence the sergeant will conduct the roll call.

4. Seated roll calls are prohibited in uniformed divisions/units.

B. ROLL CALL INSPECTION FORMATION:

A. Formations will be formed utilizing an eight (8) deputy fronts. Additional deputies shall be positioned in a second row, one on each end of the formation, squaring off the formation. Deputies will then fill in the second row, moving to a third row in the same manner when manpower dictates.
B. The lieutenant and/or sergeant conducting the roll call will be positioned directly in front of the formation, far enough so that the entire formation can be seen.

1. Additional supervisors will be positioned to the rear of the formation.

2. One additional supervisor centered to the rear of the formation.

3. Two additional supervisors square off the formation, one to each side.

C. Any persons authorized to observe or address the roll call formation will be positioned away from the formation to the left or right. They will stay at this location until after the roll call is dismissed or directed further by a supervisor.

XIV. LIEUTENANT/SERGEANT ADDRESSING THE FORMATION:

A. After having been instructed by the lieutenant to form the platoon, the squad sergeant shall command the formation in the following manner: NOTE: In the event that a ranking officer is present at the inspection formation, she/he may reserve the prerogative of inspecting and/or addressing the platoon.

1. “Platoon fall in..., Close order dress right, dress...”

   a. Officers will fall in at close interval, dress right, dress. Expandable batons will be held with a grip between the thumb and index finger of the shooting hand, vertically up and along the arm.

   b. The sergeant will verify the alignment of each rank and return to a post at the right of the formation.

2. “Ready, front – Attention to roll call”

   1. At the command of “front”, officers drop their arms to their sides and return their heads to the face front position.

   2. The lieutenant will now call the roll.

3. The lieutenant commands, “Sergeant, prepare the platoon for inspection.”

4. The sergeant commands, “Secure batons.”

   a. Baton is placed in the armpit opposite the holster.

5. The sergeant commands, “Remove magazine” (personnel who have a Glock pistol only)
a. Deputies who have Glock pistols will remove the magazine with their shooting hand, and then transfer the magazine to their non-shooting hand.
b. The magazine will be raised with the round index facing toward the inspecting supervisor.
c. **Prior to the next command being given, the lieutenant and sergeant move to the right front of the formation.**

6. The sergeant commands, **“Draw weapons.”**

a. At the command of “Draw,” deputies will unsnap their safety snap and firmly place their hand on the butt of their weapon.
b. **Deputies will not place their finger on the trigger for any reason.**

1) At the command of “weapons,” deputies will remove their weapons from their holsters and hold it head high, slightly to the front and right, or left. For left-handed persons, the barrel will remain pointed at the ceiling at all times.

7. The lieutenant, accompanied by the sergeant, will now inspect each member of the formation, **paying particular attention to the deputy’s appearance, and ensuring they are carrying a clean/loaded weapon, wearing a bullet-resistant vest, and carrying serviceable equipment.**

a. The sergeant will make note of and address any uniform/safety violations.

8. **“Conduct a safety check; ensure that your finger is outside the trigger guard.”**

a. **Deputies will again ensure that they do not have their finger on the trigger!**

9. **“Holster weapons”**

a. After placing their weapon in their holster, deputies will

1) **Snap** their holster safety strap  
2) **Return their magazine** from their non-shooting hand and place it back into the weapon.  
3) **Tug on the floor** plate of the magazine to ensure the magazine is fully inserted into the well  
4) **Conduct a hand sweep** to make sure nothing is interfering with the operation of the weapon.

B. The lieutenant will then:

1. **Instruct the formation to take out their notebooks & pens**
2. **Provide the deputy’s assignments** for the shift
3. **Read all pertinent orders, roll call complaints**
4. **Identify patterns/problem areas**
5. **Read Executive Command Staff messages**
6. **Attend to training issues**
7. **Recognize deputies for service and performance.**
8. The lieutenant will command, “Sergeant, take charge of the platoon.”

   a. The **lieutenant will exchange salutes with the sergeant.** The sergeant shall take one step forward and face left. The sergeant will command “**Platoon attention – Carry batons.**”
   b. After calling the formation to attention, the formation will be dismissed by whatever facing commands will lead the formation from the roll call room.

**IV. CIVILIAN ACCESS TO ROLL CALLS:**

A. Only the following persons will be permitted to address or attend Office of the Sheriff roll calls:

1. Any person(s) authorized by the Sheriff, Chief Deputy, or division/unit Deputy Chief.
2. Approved roll call presentations may not impede the expeditious assignment of personnel and shall occur within 15 minutes.
3. Unauthorized persons will not be permitted access to sensitive areas within a Sheriff Office facility except those normally open to the public. Authorization by the Sheriff, Chief Deputy, or division/unit Deputy Chief must be obtained to enter restricted areas.
4. Persons requesting to attend/address a roll call or tour an Office of the Sheriff covered facility should give reasonable notice to the division/unit Deputy Chief at least 24 hours prior to the roll call or inspection/tour of duty.

   a. When a request is made and the Deputy Chief is unavailable, the Commanding Officer/Captain may authorize or deny the visit request.

5. At all times, at least one deputy will accompany any person(s) inspecting/touring an Office of the Sheriff facility. The deputy must accompany the visitors while they are in areas not normally open to the public to ensure the safety of the individual and the security of the facility.

**BY ORDER OF:**

\[Signature\]

SHERIFF  DATE
DIRECTIVE: #40
SUBJECT: PERSONNEL STATUS AND ELECTRONIC COMPLIANCE
ISSUE DATE: 02-28-2020
REVISED DATE: 02-24-2021

XV. PURPOSE:

The purpose of this Directive is to establish a policy to maintain current contact information on all employees, including driver’s licenses and criminal histories and to prescribe standards for Electronic and Telephonic Compliance by members of the Philadelphia Office of the Sheriff (Office or Department).

XVI. POLICY:

It is the policy of the Office to maintain accurate data on the addresses, phone numbers, driver’s licenses, and criminal histories on all employees. Additionally, it is important that all employees properly use city issued electronic communication devices/ mediums, software or other media, i.e., text, SMS, email, cellular, websites or blogs made available through the use of devices, etc., to enhance the exchange of information and facilitate prompt responses.

A. All employees shall conform to the following Sheriff’s Office Electronic Compliance Policy and shall also adhere to Federal, State, City and Local policies.

1. **Computer accounts**: Passwords and other types of authorization are assigned to individual information users, will not be shared with others, AND will not be duplicated for use on other websites, technical resources, or electronic assets. Information users are required to protect their user ID and password and maintain the security of City information systems, Office information, and Criminal Justice Information Systems (CJIS), JNET or other criminal justice repositories they use and have legal access to.

2. **Internet**: Shall be used for informational purposes only. All Sheriff personnel are prohibited from viewing or displaying sexual images, cartoons, messages, jokes and visiting social networking or shopping sites while on duty.
3. **Email, text, SMS, etc.** All Sheriffs are to use email to communicate electronically to transfer data pertaining to specific assignments or for informational purposes only. Sheriff’s personnel are prohibited from using email to receive or send sexual images, harass, stalk, and infringe on software copyrights.

4. All employees are prohibited from using electronic devices, such as computers, cell phones, PDAs, and games (personal or otherwise) while on their assigned post and in the performance of their official duties, unless authorized.

B. Other major considerations of the Office policy include.

1. Sheriff’s Office and First Judicial District computers and communication systems are specifically prohibited from being used for sexual, ethnic, and racial harassment. Employees receiving offensive email messages will report the communications immediately to Internal Affairs.

2. Personnel Rules and Regulations on Harassment-Free Workplace, as applicable.

3. Employees should be aware that email that passes through, or is stored on, any City of Philadelphia computer network may be subpoenaed in court cases and is considered public record per the requirements of the Freedom of Information (Open Records) Act. As a public record, the public may request copies of email messages.

4. Email messages are considered the property of the Office and City, not the individual originating them.

5. Employees shall periodically purge email messages from their personal computer. Failure to do so could result in the employee’s inability to send or receive additional email messages.

6. Email signatures shall not contain quotes that may be viewed as inappropriate, offensive or have violent undertones. Acceptable email signatures include any of the following: employee's name, position/division/Office, business address, business telephone and fax number, Sheriff’s Office official motto/code/tradition and/or unaltered badge or patch image, and any pertinent disclaimers such as email and responses being subject Public Information laws or directions if receiving the email in error.

   a. Email signatures that include pictures (other than the Office of the Sheriff emblem) and/or moving or flashing text are prohibited due to increased space required in email accounts and/or servers.

7. Most email information is intended for specific individuals and may not be appropriate for general distribution. Caution shall be exercised in forwarding or transmitting general distribution email; therefore, any email intended for general distribution shall require prior permission from the Office’s Public Relations Office
8. Employees are prohibited from sending any general distribution email such as ALL CITY EMPLOYEES, OFFICE EMPLOYEES, etc., or similar groups without prior level up supervisory approval. The only exception for the requirement of prior approval shall be Intelligence Bulletins issued through the Intelligence Unit, Roll Call Training Bulletins, Vacancy Announcements, be on the lookout (BOLOs) and Everbridge messages/critical incident notifications.

   a. An employee shall send the proposed email to the PRO for review. The PRO will review the request in a timely manner and if the email is appropriate for general distribution, will forward the email to the group. If the email is inappropriate, the PRO will respond to the employee with an explanation or suggestion for change.

9. Employees shall be aware that computer files, USB (thumb) drives, external hard drives, or CD disks, and/or email attachments may contain viruses.

10. The Office of Internet Technology (OIT) Director shall ensure that all internet accessible equipment issued or utilized by the Office of the Sheriff employees employs anti-virus software prior to opening the files on their computer or attaching files to an email message.

C. Criminal Justice Information (CJI) concerns, also known as CJIS, JNet, PCIC and NCIC means information collected by criminal justice agencies that is needed for their legally authorized and required functions.

1. For purpose of this directive CJI includes Criminal History Record Information, and investigative and intelligence information, personally identifiable data, etc.

2. All employees of the Office of the Sheriff shall be responsible to familiarize themselves with the following information also incorporated herein by reference:

   https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

3. All employees will also adhere to the following CJI policies which prescribe security access guidelines regarding permissible access to CJI in any form. This includes receipt of CJI information via wireless and internet devices.

4. The following information summarize expectations relating to access to/receipt of CJI for all members of this Office:

   a. Security and access to confidential CJI is a privilege, not a right.
   b. It is the responsibility of all sworn members of the Office of the Sheriff to maintain the integrity of CJI.
c. All access to J-Net, CJIS information, PCIC/NCIC may be accessed using the last published version of the PA Justice Network Policies and Procedures manual.

d. All users who receive CJI must complete a security background check including a fingerprint check to be in the presence of any such confidential information.

e. Any persons that have or may have access to any device where CJI can be accessed must pass a security background check prior to being able to access, control, or view that sensitive information.

f. The Office of the Sheriff designated LASO and/or TAC will ensure that all employees with access to CJI who separate from the Office have all access terminated on the date of separation.

g. AUTHORIZED USE: Use of CJIS information (JNET, PCIC, NCIC, or other criminal justice or personally identifiable data) via the internet is only for authorized trusted users and agencies only. Any use of information retrieved from the aforementioned sources and used or disseminated for non-criminal justice purposes will be considered a disciplinary violation for misuse of the system and may result in disciplinary actions including administrative warnings, education-based discipline, up to including revocation from the system access and/or criminal and civil penalties.

h. AUTHORIZED DEVICES: Only approved devices are permitted access to CJI via internet. Devices accessing CJI must be issued, authorized, and managed by the Office of the Sheriff-IT Director via the agency LASO or TAC. Under NO circumstances may any non-Sheriff issued device be used to access, store, transmit or otherwise come in contact with any CJI.

a. A full review of the policies and procedures regarding "CJI-Internet access security policy" shall be conducted and signed for before access on any device is permitted.

b. The Agency JTAC is responsible for the implementation and supervision of this policy.

c. This policy including the Criminal Justice Information Security Policy [https://www.fbi.gov/services/cjis/cjis-security-policy-resource-centers](https://www.fbi.gov/services/cjis/cjis-security-policy-resource-centers) shall supersede all previous polices.

d. Any employee entrusted with access to CJI will not circumvent, change, modify or otherwise disable any technology that is deployed to either enforce or monitor compliance with these policies.

e. Employees who have access to CJI must at all times ensure their devices are secured properly secured to against unauthorized access to CJI.

f. Employees who have access to CJI must immediately report any suspected violation of this Directive.
i. Employees shall not forward any information which may be considered a myth or hoax. If the information would be of Official interest, the employee shall confirm the information and then any electronic distribution to the Office shall be approved through the Office’s PRO.

j. To ensure compliance with this Directive all employees consent to monitoring of their Sheriff issued devices by the Office to ensure compliance with this Directive.

XVII. PROCEDURE:

A. Change of address, email, and/or telephone number.

All members of the Office, sworn and civilian, will keep their current address and telephone number (cell or landline) on file with the Office for official use. Any change of address, email, and/or telephone number(s) will be reported to the employee’s immediate supervisor via official memorandum through the chain of command to the Human Resources Director and the Chief Deputy’s Aide as soon as possible, or within 24 hours.

B. Change of family status, name, and/or gender pronoun.

All members of the Office, sworn and civilian, are required to notify their immediate supervisor via official memorandum through the chain of command to the Human Resources Director and the Chief Deputy’s Aide, as soon as possible, after the occurrence of any marriage or divorce, birth or legal adoption of a child, or death of a spouse, or death of a child under 17 years of age. If an employee’s name or pronoun changes, the employee will also inform their immediate supervisor via official memorandum through the chain of command to the Human Resources Director and the Chief Deputy’s Aide within 24 hours.

C. All employees issued a city cell phone or receiving a cell phone allowance must carry the cell phone on duty and off duty. All employees opting to use a personal cell phone instead of the issued cell phone must carry their cell phone on duty and off duty. Additionally, the employee must respond, as appropriate, to all official notifications (SMS, text message, email, call) in a timely manner (under one hour).

D. All employees will receive an official city e-mail address (i.e., john.doe@phila.gov). Every employee will check their e-mail at least once every workday and respond to official e-mails in a timely manner, or by the suspense date. It is the responsibility of the employee in locations with limited terminal access to make provisions to accomplish this daily expectation; all locations covered by this

E. All employees provided phone voice mail must check for voice mail messages at least once every day they work and respond to official messages in a timely manner.
F. All employees' driver licenses and criminal histories will be checked on a monthly basis and submitted to the Sheriff/Chief Deputy by the Deputy Chief-Internal Affairs, or his/her designee to assure all drivers' licenses are valid and no unreported criminal activity has occurred. This information is due by the 1st of every month.

BY ORDER OF:

[Signature]

SHERIFF          DATE
DIRECTIVE:    #41
SUBJECT:    DOMESTIC VIOLENCE AND DEPUTIES/STAFF
ISSUE DATE:  08-01-2014
REVISED DATE:  02-24-2021

XVIII. PURPOSE:

A. The purpose of this Directive is to establish a policy governing protocols for employees who become the subject of the following: Domestic Violence Arrest, Emergency Protection Order, Temporary Protection Order, or a Final Protection Order, herein referred to as domestic violence related allegations.

1. Although an allegation of domestic violence is a criminal violation, the accusation or observations of a sworn law enforcement officer shall be enough to initiate an administrative investigation.

2. In an effort to promote transparency in law enforcement and ethical behavior among all Office of the Sheriff employees, it is the policy of this agency to assign an incident number to each domestic violence related allegations and investigate ALL complaints through the Office of the Sheriff, Internal Affairs Division.

3. Domestic violence, for purpose of this directive includes, but is not limited to:

   a. Crimes when committed by one family or household member against another:

      1) Crimes Against Persons: Assaults (of any type), Recklessly Endangering Another Person (or Children), Kidnapping, Sexual Assault, Unlawful Restraint, Rape, Stalking, Interfering with a 911 Call, Violation of a Judicial Order, etc.

      2) Property Crimes: Burglary, Defiant Trespass, Trespass, Criminal Mischief, Vandalism

4. Family or household members means:

   a. Spouses
   b. Former spouses
c. State registered domestic partners

d. Former state registered domestic partners,

e. Persons with a child in common regardless of whether they have been married or have lived together,

f. Adult persons related by blood or marriage

g. Adult persons presently residing together or who have resided together in the past

h. Persons sixteen years of age or older who are presently residing together or who have resided together in the past and who have or have had a dating relationship

i. Persons sixteen years of age or older with whom a person sixteen years of age or older has or has had a dating relationship

j. Persons with a biological or legal parent-child relationship, including stepparents and stepchildren and grandparents and grandchildren.

k. Dating relationship means a social romantic relationship. In making this determination include:

1) The time the relationship has existed
2) The nature of the relationship
3) The frequency of interaction between the parties.

5. **Victim:** means a family or household member subjected to domestic violence.

XIX. **POLICY:**

A. Once a deputy/staff member of the Philadelphia Sheriff’s Office has been notified that he/she is the defendant in any Emergency Protection Order, Temporary Protection Order, or a Final Protection Order the deputy/staff member will surrender his/her duty issued weapon, and ammunition. Additionally, the deputy/staff member will be reassigned to administrative duties.

1. The employee will contact the ranking on duty supervisor immediately after being served with a protection order.

2. The employee shall comply with all the provisions of the order. The employee will surrender all privately-owned firearms to the Philadelphia Sheriff’s Office Firearms Unit located at 100 S Broad Street 5th Fl. If it is after regular working hours or on weekends, firearms shall be surrendered to the highest-ranking supervisor at CJC 1301 Filbert St.

3. When relinquishing his/her firearms, the deputy/staff shall provide a copy of the order that was served to them.

B. When a Deputy/staff responds to any other domestic incident involving a Sheriff’s Office member, the responding deputy shall notify the on duty/on call Sheriff’s Office supervisor.
C. The on duty/on call supervisor upon notification of a domestic incident shall notify the following persons via Everbridge Notification: Sheriff, Chief Deputy, Undersheriff, the Internal Affairs Division, and applicable Deputy Chief or Chief Inspector in the involved employees’ chain of command.

D. Commanding Officers responding to calls for domestic violence or protection From Abuse orders served on Sheriff’s Office deputies/staff will be cognizant of this policy and share the same responsibility delineated in II-C for notifications.

E. The sworn deputy who is the subject of the order will surrender their badge, Sheriff’s Office identification and PCCD Certification Card to the responding supervisor or commanding officer. S/he will be prohibited from taking law enforcement action until the case is adjudicated and will therefore be reassigned to a non-law enforcement function.

NOTE: Notification to a Supervisor or Internal Affairs regarding any order does not imply wrongdoing on the part of the involved employee.

XX. **RESPONDING SUPERVISOR/COMMANDING OFFICER**

A. The responding supervisor/commanding officer will:

1. Review the order and immediately seize any issued firearms and ammunition in the employee’s possession and privately owned firearms and ammunition, if the employee is in the possession of any. A copy of the order will also be surrendered.

2. Ensure the employee relinquishes any city owned or personally firearms and ammunition.

3. Fully explain to the employee the contents of the order.

4. During business hours, if the order is either an Emergency or Temporary Order, be responsible for securing the firearms and ammunition until the Firearms Unit Officer arrives. If the order is a Final Protection Order, the commanding officer shall likewise maintain control of all weapons and ammunition until surrendered to the Firearms Unit Officer.

5. During off-work hours or weekends, reassign the deputy/staff member to report on the next workday to administrative duties at 100 S. Broad Street; position will be determined by the Chief Deputy, Undersheriff, or their designee.
1. The deputy will be in **conservative business casual** attire while working, e.g., pants, khakis, a collared shirt, and shoes. TENNIS SHOES, SNEAKERS, BDUs, SKINTIGHT TOPS, HIGH HEELS MINI SKIRTS, TANK TOPS, T-SHIRTS, are inappropriate and therefore not in compliance with this directive.

2. Evaluate the nature of the order and document whether the nature of the order, res gestae (thing which may be admissible in court) statements, and officer observations necessitate subjecting the employee to a Fitness for Duty/Psychiatric Examination or making a mandatory or voluntary referral to the Employee Assistance Program.

3. Personally, complete an Incident Report, to include their personal observations, the employee’s name, badge, and payroll number, including a specific reference to taking possession of the employee’s firearm(s) and ammunition. Ensure the preparation of the report includes the full names of all involved parties, the Order number, and all relevant provisions in the Order. The employee will be given a copy of the incident report as a receipt on scene, if possible.

B. The Internal Affairs Captain will be responsible for monitoring the outcome of all domestic violence related hearings and, if applicable, recommending the deputy/staff member restoration to normal duties via closure of the internal investigation and a memorandum up the chain of command to the Sheriff.

1. If the Internal Affairs Division investigation finds the employee culpable, the Sheriff can impose restrictions upon the employee, until she/he has completed an EAP. Internal Affairs Division finds are not dependent upon those of a Court or any other governmental body. This directive does not exclude the employee from other disciplinary actions, due to her/his violations of Sheriff’s Office policy, during the Domestic Violence incident.

XXI. DOMESTIC VIOLENCE COUNSELING AND REFERRAL LIST:


B. Pennsylvania Statewide Automated Victim Information and Notification (PA SAVIN): an available service offered by the Pennsylvania District Attorneys Institute. This is a free service which alerts the victim to important custody information on a specific offender who is in jail. Once a victim signs up by calling 1-866-972-7284 and selects a four (4) digit PIN code, the system calls them at a designated phone number or e-mail to notify them if the offender is released, transferred or escapes. The PA SAVIN service includes offenders under the
supervision of county jails, state prisons, and state parole but does not include offenders who are released directly from the police district. The complainant can also register through the official website at www.pacrimevictims.com

C. Counseling Services:

1. **Lutheran Settlement House:** bi-lingual Domestic Violence Program 215-426-8610-Individual counseling and support groups in English and Spanish.
2. **Congreso de Latinos Unidos:** Latina Domestic Violence Program 215-763-8870, Counseling and support for English and Spanish speaking women and children.
3. **Women in Transition:** 215-751-1111, domestic Violence and/or substance abuse counseling for women.
4. **Women Organized Against Rape:** 215-985-3333, 24-hour hotline for sexual assault victims.
5. **Menergy:** 215-242-2235, program for abusive men.

D. Legal Services:

1. **Philadelphia Legal Assistance:** 215-981-3800, legal assistance and representation for domestic violence, child support, child custody, divorce, unemployment, bankruptcy, and public benefits.

2. **Women Against Abuse Legal Center:** 215-686-7082, Legal assistance and representation, court accompaniment for domestic violence, child support, and child custody.

3. **Women’s Law Project:** 215-928-9801, legal information on domestic violence and family law, telephone counseling only; no representation.

**XXII. This Directive is effective immediately.**

BY ORDER OF:

[Signature]

SHERIFF DATE
Philadelphia Sheriff's Office

DIRECTIVE: #42
SUBJECT: OFFICE RELATIONSHIPS
ISSUE DATE: 01-16-2020
REVISED DATE: 02-24-2021

XXIII. PURPOSE:

A. The purpose of this Directive is to help employees avoid the conflict of interests that arises whenever an employee disregards the public interest in favor of other interests such as personal, family or business relationships. A conflict may exist whenever an employee, because of one of these relationships, becomes incapable of impartially performing their official duties. A conflict of interest may result in favorable or unfavorable actions whenever decisions are based on personal, family or business relationships.

B. The avoidance of conflict is particularly important for all levels of command and supervision with their subordinates by rank or classification especially within the same chain of command or workgroup. The authority given a supervisor over a subordinate is a responsibility entrusted to that supervisor by the Sheriff of the County/City of Philadelphia.

XXIV. POLICY:

A. It is the policy and extended responsibility expectation of this Department that every decision made by a supervisor be totally objective, impeccably fair, and above all, devoid of any favorable or unfavorable actions due to any relationship between the supervisor and the subordinate. Also, when a supervisor has a personal, family or business relationship with a subordinate, any one of these relationships may result in a negative perception by others and the motive for decisions made by the supervisor may become suspect and compromise the integrity of all involved. This could lead to a disruptive work environment, reduced productivity, and a decline in overall morale.
B. Definitions

1. For purposes of this order, a supervisor is defined as a person who has command, control, direction, or supervision over others.

2. For purposes of this order, workgroup includes a division, section, facility, or unit.

3. A supervisor/subordinate work relationship exists when, within the chain of command or workgroup, one employee commands, controls, directs, supervises, or may influence another employee's terms, conditions, or privileges of employment.

XXV. PROCEDURE:

A. When any employee determines a conflict exists or may exist due to personal, family or business reasons, the employee shall immediately contact their immediate supervisor or commander. The supervisor or commander contacted will resolve the situation in accordance with the provisions of this order and prepare a memorandum through the chain of command to the Chief Deputy.

B. An employee required to report a relationship in which they are involved or one involving other may find it uncomfortable or awkward to report the matter to their immediate supervisor. Therefore, employees may report the matter to any ascending-level supervisor in their chain of command, EAP, or the female employees’ coordinator. The person receiving the information shall immediately report the matter to the appropriate deputy chief, Undersheriff, or the Chief Deputy.

C. Supervisors making personnel assignments or selecting personnel for in-house vacancies shall not assign or select any employee for an assignment in which a personal, family or business relationship exists, when such relationship would constitute a conflict as described by this order.

XXVI. PERSONAL RELATIONSHIPS:

A. A personal relationship in and of itself is not inappropriate. The department shall exercise due respect for the right of personal associations and privacy of all employees of this organization. However, all decisions by a supervisor must be viewed as fair, objective, and impartial. Therefore, when personal relationships between supervisors and subordinates that create a conflict occur in the workplace, there is cause for concern by the department. These relationships must be addressed and resolved as directed by this order in the interest of maintaining an objective and impartial working environment for all employees.

1. A personal relationship means a sexual, romantic, or dating relationship or any interpersonal relationship or social activity in which there is a real or potential non-platonic interest between two employees.
2. Supervisors shall not maintain or continue in a personal relationship with any subordinate in their chain of command or within their same workgroup.

3. When a personal relationship exists or occurs between a supervisor and subordinate who are in the same chain of command or within the same workgroup, the involved supervisor shall immediately inform their immediate supervisor. The appropriate division chief inspector, deputy chief or manager shall also be notified and shall ensure one of the involved employees is immediately reassigned to a position in which the supervisor/subordinate relationship conflict no longer exists. The Chief Deputy or the Undersheriff shall be notified to ensure the action taken is appropriate. Transfers based on personal relationships shall be made in accordance with existing transfer procedures, but in any case, the Chief Deputy shall ensure immediate and appropriate action is taken to preclude the continuance of the personal relationship conflict in the chain of command or within a workgroup.

4. If any supervisor has any indication that a personal relationship as defined in this directive exists or is developing which would be a conflict, the supervisor shall ask reasonable questions relating to the matter as it involves the workplace. If it is determined that a conflict does exist, the action as described in this directive (IV.A.3) shall be taken. If it is determined a relationship exists and the supervisor involved in the relationship has not reported it as required by this directive, a disciplinary investigation will be initiated in accordance with existing procedures for such investigations.

5. An employee who has a personal relationship with any employee shall not contact any person within the department for the purpose of directly or indirectly influencing any decisions concerning that employee’s terms, conditions, or privileges of employment.

XXVII. FAMILY RELATIONSHIPS:

A. Family members may be employed and work together within the department. A family member shall not occupy a position which could affect another family member’s employment, conditions or terms of employment, or other management-related personnel action.

1. A family relationship means immediate family such as spouse, child, stepchild, parent, stepparent, grandparent, grandparent-in-law, grandchild, parent-in-law, brother, sister, brother or sister-in-law, and son or daughter-in-law.

2. If a family relationship exists or occurs between a supervisor and subordinate who are in the same chain of command or workgroup, the supervisor shall immediately inform their commander or manager. The commander or manager shall ensure one of the involved employees is immediately reassigned so that the
supervisor/subordinate relationship conflict no longer exists. The Deputy Chief of the Unit shall be notified to ensure the action taken is appropriate. Transfers or promotions based on family relationship conflicts shall be made in accordance with existing transfer procedures but, in any case, the Bureau Deputy Chief shall ensure immediate and appropriate action is taken to preclude continuation of the family relationship conflict in the chain of command.

3. An employee who has a family relationship with any employee shall not contact any person within the department for the purpose of directly or indirectly influencing any decisions concerning that employee’s terms, conditions, or privileges of employment.

XXVIII. BUSINESS RELATIONSHIPS:

A. Public trust requires that employees avoid even the appearance of a conflict between their professional responsibilities and their personal business interests.

1. For purposes of this order, a business relationship means any association of two or more persons to carry on a business for profit; the association of two or more persons to own and/or to operate a business venture as equal members; two or more persons who have a financial or pecuniary interest, directly or indirectly, in a business, service, or contract; or, any employee of the department who is employed directly or indirectly with any company or individual that does or seeks to do business with the city.

2. Supervisors shall not enter or continue a business relationship with members of their chain of command. If a pre-existing business relationship exists or should a transfer create a business relationship conflict, the involved supervisor shall immediately inform their commander or manager. The commander or manager shall ensure one of the involved employees is immediately reassigned so that the supervisor/subordinate business relationship no longer exists. The concerned deputy chief shall be notified to ensure the action taken is appropriate. Transfers on the basis of business relationship conflicts shall be made in accordance with existing transfer procedures but, in any case, the Chief Deputy shall ensure immediate and appropriate action is taken to preclude continuation of the business relationship conflict in the chain of command.

1. Any employee who has a business relationship with any other employee shall not contact any person within the Office for the purpose of directly or indirectly influencing any decisions concerning that employee’s terms, conditions, or privileges of employment.

2. No employee shall have a business relationship with any company or person that does or seeks to do business with the city.
XXIX. EMPLOYEE APPLICANTS, TRAINEES, AND PROBATIONARY EMPLOYEES:

A. Employee applicants, trainees, and probationary employees in their selection, employment and training are especially vulnerable to implied threats or coercion, as they are constantly being evaluated.

B. Regular and permanent employees are in a position to exert influence over and may participate in some way in the selection, training or evaluation of employee applicants, trainees, or probationary employees. Therefore, regular, and permanent employees shall not initiate any personal or business relationship with any applicant, trainee, or probationary employee.

C. Employees who have a pre-existing personal, family, or business relationship with an applicant, trainee, or probationary employee shall refrain from making any decisions regarding the application, selection, training, or probationary employee status of the individual.

1. Employees who have such a pre-existing personal, family, or business relationship shall immediately inform their commander or manager.

2. The commander or manager shall ensure that the involved employee make no decisions that may directly or indirectly affect the application, selection, trainee, or probationary employee/office process.

D. Employees who do share a personal, family, or business relationship with any employee applicant, trainee, a probationary officer or employee shall not contact any person within the Office or any person involved in the selection, training, or evaluation process for the purpose of directly or indirectly influencing any decisions concerning the subject individual's terms, conditions, or privileges of employment.

E. Employees who are in their entry-level trainee or probationary status are

A. Prohibited from establishing a personal or business relationship with any other employee of the department.

B. Shall immediately report to their division commander or manager any actions by any regular or permanent employee that may conflict with this directive.

BY ORDER OF:

[Signature]

SHERIFF DATE
Philadelphia Sheriff's Office

DIRECTIVE: #43
SUBJECT: OFF DUTY LAW ENFORCEMENT ACTIONS
ISSUE DATE: 04-14-2020
REVISED DATE: 02-24-2021

XXX. PURPOSE:

A. The Philadelphia Office of the Sheriff has the management right to regulate the law enforcement related off-duty employment of its employees. This policy applies to the off-duty employment of all sworn employees.

B. The safety of sworn members and others in the immediate area shall be the paramount concern when deciding to take off-duty law enforcement action. Also, any action taken off-duty must always be consistent with Federal, State and Philadelphia Sheriff’s Office directives, policies, and procedures. All off-duty law enforcement actions, regardless of the jurisdiction of occurrence, are subject to review, administrative and criminal investigation, and disciplinary actions, if warranted.

C. All off-duty law enforcement actions reflect upon the integrity of the individual sworn-member as the entire Philadelphia Sheriff's Office. Therefore, all off-duty law enforcement actions must be beyond reproach and avoid even the appearance of any improprieties. As such, sworn-members shall NOT take any off-duty law enforcement action in any minor family or neighborhood disputes, summary offenses, or traffic violations, unless such action is necessary to prevent bodily injury, serious bodily injury, or death. Sworn members shall call emergency 9-1-1 in these situations.

D. In most off-duty situations, the safest and tactically superior action is to simply call emergency 9-1-1 and provide detailed information for the responding on-duty law enforcement officer/deputy. There is no cowardice in refraining from engaging in off-duty law enforcement action when not properly prepared or equipped. It is simply proper deputy safety tactics to protect yourself, as well your family.

II. POLICY:

A. It is the policy of the Philadelphia Office of the Sheriff to ensure the safety of sworn members and their families. Sworn members are however, expected to assist on-duty
law enforcement officers when necessary. Sworn members in "off-duty" status are required to use their best judgment when responding to an incident while off duty. If the officer cannot in his best judgment effectively assist, then they are required to call 9-1-1 emergency if they witness a crime in action. However, this restriction shall NOT be construed or interpreted to restrict any sworn member, regardless of duty status, from defending themselves, their families, or another deputy/officer, if necessary, from bodily injury, serious bodily injury, or death.

B. Sworn members using intoxicants or taking any medications that may impair judgment or physical abilities are prohibited from taking any off-duty police actions, other than calling emergency 9-1-1. However, this restriction shall NOT be construed or interpreted to restrict any sworn member from defending themselves, their families, or another deputy/officer, if necessary, from bodily injury, serious bodily injury, or death.

III. PROCEDURES:

A. Most times, an off-duty deputy sheriff lacks body armor, may be unarmed, and usually lacks backup or communications. In cases where the deputy observes behavior warranting immediate intervention, the deputy should dial emergency 9-1-1, identify themselves to dispatch and the parties involved, including arriving law enforcement officers by verbalizing that she/he is a law enforcement officer AND displaying identification card and or badge, if practical. 

B. Upon arrival of the on-duty law enforcement officer, the initially involved off-duty deputy will turn over responsibility of the scene to the on-duty officer. If the off-duty deputy is effectuating an arrest or initiating a police action, the deputy will be a Complaint or Incident Report (75-48) and will complete any other forms required by the Philadelphia Police Department or the local jurisdiction. The on-duty Sheriff’s Office supervisor shall be notified at CJC 215-683-7900.

IV. REPORTING REQUIREMENTS:

A. For every off-duty arrest or law enforcement action, the on-duty Sheriff’s supervisor shall be notified at the CJC.

B. The on-duty Supervisor shall notify the Command Staff via Everbridge and notify the Internal Affairs Unit via telephone with the name, payroll number, assignment, and pertinent details of the incident.

C. When a deputy is injured as a result of any off-duty actions or arrest, the Sheriff or his designee shall be notified via Everbridge, as well as the Internal Affairs Unit via telephone. Internal Affairs will track and record all off-duty arrests or law enforcement actions, serving as the office’s central review and repository unit. A notification to Internal Affairs does not imply wrongdoing on the part of deputies who take police action off-duty. In the cases where Internal Affairs will investigate,
the involved deputy will be notified that his/her report is not necessary.

D. Any sworn member of the Sheriff's Office, who makes an arrest outside the city and county of Philadelphia, shall contact the on-duty Sheriff's supervisor as soon as possible.

E. Whenever sworn member of the Office of the Sheriff is arrested the involved person will notify the on-duty Sheriff's Office supervisor. The supervisor receiving the notification will follow all sections of IV-A-E.

1. The on call IAD Supervisor will retrieve the arrested deputy's badge and firearm immediately.

2. The involved deputy will be immediately placed on restricted duty and reassigned by their respective Deputy Chief until the administrative or criminal investigations are completed.

3. Restricted duty shall entail the prohibition by this directive from taking any law enforcement actions until the restriction is removed by the Sheriff, or her designee.

BY ORDER OF:

[Signature]

SHERIFF Date
Philadelphia Sheriff’s Office

DIRECTIVE: #44
SUBJECT: PA COMMISSION ON CRIME AND DELINQUENCY EDUCATION AND TRAINING PROGRAM
ISSUE DATE: 03-17-2020
REVISED DATE: 02-17-2021

XXXI. BACKGROUND:

A. The Pennsylvania Commission on Crime and Delinquency (PCCD or the Commission) and the Sheriff and Deputy Sheriff Education and Training Board (the Board), under the authority granted by Act 10 of 1998, has established guidelines to administer the Board’s training programs.

B. Under P.S. § 2101 (2014) The act governing the powers of a Sheriff and Deputy Sheriff in Pennsylvania is known and may be cited as the Sheriff and Deputy Sheriff Education and Training Act.

C. A deputy sheriff, who has completed the deputy sheriff's basic training course provided under the Deputy Sheriff's Education and Training Act, 71 P.S. § 2101 et seq., the driving while under the influence modules given to municipal police officers under former 53 P.S. §§ 740 to 749.1 (now 53 Pa.C.S. §§ 2161 to 2171), and training in field sobriety test administration, qualified as a "police officer" for purposes of enforcing the Vehicle Code under the rationale of the holding in Commonwealth v. Leet, 537 Pa. 89, 641 A.2d 299 (1994); accordingly, a driver's challenge to the deputy's authority to make a warrantless arrest was unsuccessful in an appeal of a one year license suspension for refusal to submit to a breathalyzer test, as provided for under 75 Pa.C.S. § 1547(a)(1). DOT, Bureau of Driver Licensing v. Kline, 559 Pa. 646, 741 A.2d 1281, 1999 Pa. LEXIS 3784 (1999).

XXXII. REQUIREMENTS:

1. Definitions:
   b. Board: The Sheriff and Deputy Sheriff Education and Training Board.

2. The Board, with the review and approval of the Commission, has established a continuing education program for all sheriffs and deputy sheriffs, which shall include not less than 20 hours of continuing education every two years, concerning subjects the Board may deem necessary and appropriate for the continuing education and training of sheriffs and deputy sheriffs.

3. The board, with the review and approval of the commission, shall:

   a. Establish, implement, and administer the Sheriff and Deputy Sheriff Education and Training Program according to the minimum requirements set forth in the act.

   b. Establish, implement, and administer requirements for the minimum courses of study and training for sheriffs and deputy sheriffs.

   c. Establish, implement, and administer requirements for courses of study and in-service training for sheriffs holding office and deputy sheriffs appointed prior to the effective date of this act.

   d. Establish, implement, and administer requirements for a continuing education program for all sheriffs and deputy sheriffs concerning subjects the board may deem necessary and appropriate for the continued education and training of sheriffs and deputy sheriffs.

   e. Approve or revoke the approval of any school which may be utilized to comply with the educational and training requirements of the act.

   f. Establish the minimum qualifications for instructors and certify instructors.

   g. Consult and cooperate with universities, colleges, law schools, community colleges and institutes for the development of specialized courses for sheriffs and deputy sheriffs.

   h. Promote the most efficient and economical program for sheriff and deputy sheriff training by utilizing existing facilities, programs and qualified State and local personnel.

   i. Certify sheriffs and deputy sheriffs who have satisfactorily completed the basic education and training requirements of this act and issue appropriate certificates to them.

   1) Revoke the certification of sheriffs and deputy sheriffs
2) Reinstate previously revoked certifications of sheriffs and deputy sheriffs where the board finds that the circumstances which led to the revocation of certification are no longer an impediment to certification.

j. Make rules and regulations and perform other duties as may be reasonably necessary or appropriate to administer the act.

k. Make an annual report to the Governor and to the General Assembly concerning the administration of the Sheriff and Deputy Sheriff Education and Training Program, the activities of the board, and the costs of the program.

4. Training program

a. The Sheriff and Deputy Sheriff Education and Training Program shall include appropriate training for not less than 760 hours which content and hours of instruction shall be determined by the board, subject to the review and approval of the commission.

b. As a law enforcement officer, a deputy sheriff is authorized under Pa. R. Cr. P. 504 to be an affiant on a criminal complaint against a defendant...; (sic) provided the sheriff completed all of the training required of a deputy sheriff, including all continuing education updates pursuant to 71 P.S. § 2106, so s/he does not have to complete training under 53 Pa.C.S. 2161 et seq. in order to be authorized to carry out his or her legal duties.

5. Continuing Education

a. The board, with the review and approval of the commission, shall establish a continuing education program for all sheriffs and deputy sheriffs, which shall include not less than 20 hours of continuing education every two years, concerning subjects the board may deem necessary and appropriate for the continued education and training of sheriffs and deputy sheriffs.

b. See I, C-2.

6. Sheriff Training Certification Requirement

a. It shall be the duty of any sheriff elected after the effective date of this section and not holding certification as either a deputy sheriff or sheriff on the first Monday in January next following the election, during the sheriff's term of office:

1) To obtain the education and training as provided in section 5, subject to any reduction in hours as provided in subsection (c).
2) To meet the requirements for continuing education after certification.
3) To obtain reinstatement of a previously revoked certification, if applicable.

b. In the case of a county which has adopted a home rule charter which provides for the appointment of the sheriff, a sheriff appointed after the effective date of this section shall obtain certification under this section within 18 months of appointment.

c. Continuing education: Every sheriff shall, while in office, meet the requirements for continuing education established by the board, with the review and approval of the commission.

d. Prior education, training, or experience: The board, with the review and approval of the commission, shall have the authority and the discretion to reduce the hours of education and training required in for sheriffs required to receive education and training who, because of prior education, training or experience, have acquired knowledge or skill equivalent to that provided by the program.

e. Sheriffs in office: Any sheriff holding office on the effective date of this requirement (section of law) shall be deemed to have satisfied the requirements for training and shall receive certification from the board. From the date of the certification under this subsection, sheriffs shall be subject to continuing education as provided in subsection 5b.

f. Ineligibility: Any sheriff failing to receive and maintain certification as provided in this section shall be ineligible to be on the ballot for the office of sheriff for any term subsequent to that referred to in subsection-a.

g. Vacancies:

1. Any person appointed to fill a vacancy in the office of sheriff shall be certified or, in the alternative, obtain and maintain certification during the term for which the person is appointed in accordance with subsection-a.

   i. Any person appointed to fill a vacancy in the Office of the Sheriff who does not fulfill the requirements of subsection-(a) shall be ineligible for subsequent election as provided in subsection-f.

2. No person appointed to fill a vacancy in the Office of the Sheriff where the balance of the unexpired term is less than one year shall be subject to the requirements of paragraph g-1. However, a person who is elected to a term as sheriff immediately following the person's previously appointed term of less than one year is subject to the requirements of subsection (a).
h. Purpose and Legislative Intent: It is hereby declared to be a public policy of
this Commonwealth that sheriffs receive and maintain education and
training equivalent to that required by law of deputy sheriffs in order to
preserve the safety of county facilities, employees and residents. It is
further declared that a newly elected sheriff has an opportunity to satisfy the
requirements of the act during the sheriff's first term, notwithstanding past
training, and experience.

XXXIII. HISTORY:

A. Act 2014-114 (H.B. 1772), P.L. 1006, § 6, was approved on July 9, 2014.

B. Application of ACT 2014-114: Every sheriff of this Commonwealth shall assure that
each full-time or part-time deputy employed by the sheriff who has less than five
years of experience receives the training delineated within this directive.

1. Diploma: No person shall be employed or appointed as a deputy sheriff unless the
person is a high school graduate or has received a secondary school diploma
based on general education development (GED).

2. Prior Education, Training or Experience: The board, with the review and approval
of the commission, shall have the authority and the discretion to reduce the hours
of education and training required in section II, 5 for those deputy sheriffs
required to receive education and training who, because of prior education,
training or experience, have acquired knowledge or skill equivalent to that
provided by the program.

3. Certification requirement for Continued Compensation:

a. Any person hired as a full-time or part-time deputy sheriff who has less than
five years of experience on the effective date of this act shall, at the end of
two years from the effective date of this act, be ineligible to receive any
salary, compensation or other consideration or thing of value for the
performance of duties as a deputy sheriff unless the deputy sheriff has met all
of the requirements established pursuant to the act and has been duly certified
as having met those requirements by the board, with the review and approval
of the commission, unless the deputy sheriff is granted additional time to
complete training by the board, with the review and approval of the
commission.

b. Any new deputy hired by the sheriff after July 1, 1985 shall have one year in
which to complete training.

c. Any full-time or part-time deputy sheriff who fails to meet and fails to be
certified as having met the requirements for continuing education established
by the board, with the review and approval of the commission, shall be
ineligible to receive any salary, compensation or other consideration or thing of value for the performance of duties as a deputy sheriff.

XXXIV. **REVOCATION OF CERTIFICATION:**

A. Revocation of Deputy Sheriff Certification: The board shall revoke the certification of any deputy sheriff for one or more of the following:

1. Conviction for a felony or misdemeanor of the first or second degree.
2. Where the board determines the person was dismissed for cause from employment as a deputy sheriff.
3. Where the board determines the person is physically or psychologically unfit to perform the duties of the office.
4. Where the board determines the person has committed misconduct which makes the person unfit to perform the duties of the office, including:
   a. Submission to the board of a document that the deputy knows contains false information, including fraudulent application.
   b. Cheating on board examinations or skill tests.

B. Revocation of Sheriff Certification: The board shall revoke the certification of a sheriff only after the sheriff is removed from office. Nothing in this act shall be interpreted as providing grounds for removal of a sheriff from office, except as provided for by Article VI of the Constitution of Pennsylvania.

C. Notification by Sheriff: In the case of a deputy sheriff, it shall be the responsibility of the sheriff to notify the board within 15 days of the occurrence of an event described under sub-section (IV-A).

D. Notification by County Commissioners (in the City and County of Philadelphia, it is City Council): In the case of a sheriff, it shall be the responsibility of the Council to notify the board within 15 days of a sheriff's removal from office.

E. Regulations: The board shall establish, with the approval of the commission, regulations providing for the following:

1. Notice of a revocation and the right of sheriffs and deputy sheriffs to request a hearing.
2. Standards and guidelines for application for recertification following revocation.

**BY ORDER OF:**

[Signature]

SHERIFF        DATE

282
XXXV. **POLICY:**

A. It is the policy of the Philadelphia Office of the Sheriff to protect the rights of all citizens under the 1st Amendment of the US Constitution ensuring “Freedom of Speech” and the “Right to Peaceably Assemble.”

B. Deputy Sheriffs are reminded in this directive to respect the public’s right to express opinions concerning the actions of City Council, other branches of government, and limited rights at Sheriff’s Sales. A member of the public may quietly and discreet request from the Deputy-In-Charge of Real Estate to have an undeclared interest announced at a Sheriff’s Sale. The Real Estate Deputy-In-Charge shall consult with the Undersheriff to determine if the request shall be granted. It is important for the deputy to use discretion and to strike the appropriate balance when evaluating any disruption or impingement upon the rights of those involved in an official meeting being held by an individual member, a committee, or the entire City Council body. Therefore, upon warning, active disruptions of public meetings and acts of disorderly conduct, threatening, or violent behavior will not be tolerated in order to expressly preserve the rights of all in attendance.

C. Any individual or group actively disrupting a meeting after being warned to cease the disrupting behaviors may be forcibly removed and criminally prosecuted (at minimum) under the following sections of Title 18 PA statutory laws:

1. **Section 5508: Disrupting Meetings**
   - Punishment: Imprisonment-Not to exceed one (1) year
   - Fine: Not to exceed $2,500.00

2. **Section 5503: Disorderly Conduct**
   - Punishment: imprisonment-Not to exceed one (1) year
   - Fine: Not to exceed $2,500.00
XXXVI. **PROCEDURE:**

A. The following delineation of duties and powers shall serve as the model for enforcement in removing persons who actively disrupt public meetings:

1. **City Council-Sergeant at Arms**
   The Sergeant at Arms has the primary responsibility to maintain order within the City Council Chambers. Upon the incidence of any disruption of a Council Session or Meeting, the Sergeant at Arms will verbally request the disruptor(s); warning them to either cease the disruption or leave the session or meeting.

2. **Sheriff’s Deputies**
   a. Should the disruptor(s) decline to adhere to either cease the disruption, or to leave, the Council President or his/her designee shall serve as the complainant for the deputy’s incident report and may direct the deputy sheriff to forcibly remove the disruptor(s). A report will be prepared whether the disruptor(s) is warned, forcibly removed, and/or arrested.
   
   b. The deputy may remove an individual if there is an immediate danger of death or serious bodily injury pursuant to PA CS. Title 18, Chapter 27.
   
   c. The deputy may remove an individual if they receive a lawful order from the Fire Marshall.
   
   d. The deputy may remove an individual if a person enters posted and designated as restricted/shall require proper identification (credentials or identification for the City Council Members, Mayor, Council/Mayoral Staff and/or designees).
      
      1) Any person(s) found by Office of the Sheriff Deputies in restricted areas (i.e., Council Floor beyond railings) shall be immediately removed by deputies and/or police.
   
   e. The P.S.O. Supervisor will be notified by the arresting deputy; the supervisor will send a notification to Executive Command Staff via Everbridge.
   
   f. **Will adhere to the current P.S.O. Use of Force Policy.**
   
   g. Any such removal shall be documented in an Office of the Sheriff Incident report, use of force report, I.A.D. report, if applicable.

XXXVII. **MISCELLANEOUS:**

284
A. Occupancy Rules

1. Shall be based upon the Rules, Regulations, and Codes of Philadelphia License and Inspections and Fire Code.

B. Posters/Banners

1. Only posters and banners made of cardboard and paper will be permitted inside of City Council Chambers.

2. Wooden and metal attachments are NOT PERMITTED.

C. Additional Prohibited Conduct within City Council Chambers

1. No objects that may be used as weapons are allowed in Council Chambers.

2. No affixing or taping of posters or signs on walls or glass in the gallery balcony area is permitted.

3. Members of the public must turn off all cell phones and communication devices that emit sound.

D. Philadelphia Police Department Civil Affairs Unit

1. May be first to respond to the location of a civil disturbance or civil injunctions and are permitted to make arrests for violations of the PA Crimes Code committed in their presence.

2. **May not legally enforce civil injunctions without an Office of the Sheriff Deputy.**

3. Assists the Office of the Sheriff by maintaining open lines of communication with protest leaders.

E. Public Accommodations Defiant Trespass Situations

1. The Philadelphia Sheriff's Office is tasked with the duty of keeping peace and order in the facilities of other governmental partners. Often deputes arise between employees of these agencies and the public and deputes are asked to eject members of the public from such facilities by our governmental partners. All deputes shall be aware of the following protocols before ejecting any persons out of any public place. Observance to these protocols shall always be in force, but particularly in places where governmental tribunals take place. Extra care shall be taken in these instances because in these less than formal
tribunals members of the public may lose some type of property if they cannot defeat the claims made against them.

2. Deputies employed by the Philadelphia Sheriff’s Office shall take careful note and observe that the Philadelphia Home Rule, Chapter 9; Section 1102 defines Public Accommodations as any place, provider or public conveyance, whether licensed or not, which solicits or accepts the patronage or trade of the public or whose goods, services, facilities, privileges, advantages or accommodations are extended, offered, sold or otherwise made available to the public; including any public agency or authority; or other instrumentality of the Commonwealth.

3. All Philadelphia Sheriff’s Office employees shall be familiar with and enforce Chapter 9; section 1106 of the Philadelphia Home Rule Charter, which makes it illegal to deny or interfere with public accommodations opportunities due to the subject’s race, ethnicity, color, sex, sexual orientation, gender identity, religion, national origin, ancestry, disability, marital status, familial status, or domestic violence victim status.

4. Deputies employed by the Philadelphia Sheriff’s Office shall also observe that the Supreme Court of the United States of America has ruled in the Mullane v. Central Hoover Bank case that the Constitutional requirement of “due process of law” has a minimum of three (3) components: 1) Notice; 2) an opportunity to be heard and 3) an impartial tribunal.

5. When confronted with a defiant trespass in a public accommodations’ situation, the Deputy shall first attempt to de-escalate and mediate the disturbance between parties.

6. If the deputy is unable to mediate the situation, the deputy shall request that the complainant tell the subject to vacate the premises in front of the deputy.

7. The deputy shall ensure that the subject understands the complainant’s call for her/him to vacate the facility. In this way, the deputy witnesses for her/himself the subject refusing to honor a legitimate request to leave the facility.

8. Before making an arrest, the deputy may call a supervisor or crisis intervention trained deputy to the scene to help de-escalate the state of affairs.

9. If the deputy believes that according to Chapter 9; section 1106 of the City’s Home Rule Charter or the Supreme Court Ruling, Mullane v. Central Hoover Bank the subject rights were violated, the deputy shall instruct the subject to file a complaint with the Philadelphia Commission on Human Relations at 601 Walnut St., Suite 301. The deputy shall provide the subject with her/his
name, badge number, supervisor's name and contact and shall respond appropriately to any summons or subpoena from the Commission.

10. If after all the proceeding protocols have been exercised and the subject still refuses to vacate the premises, the deputy shall have the complainant sign off on an Intention to Prosecute Form before any arrest. Once the form has been signed the deputy shall make one last attempt to order the subject to vacate the premises. If the subject refuses, the deputy shall effectuate an arrest. It shall be noted that back up can be called in at anytime during the Public Accommodation Defiant Trespass process.

11. Nothing in this directive forbids the deputy from arresting the subject for any crimes, which may be committed in front of her/him.

BY ORDER OF:

[Signature]

SHERIFF DATE

287
DIRECTIVE: #46
SUBJECT: SOCIAL MEDIA
ISSUE DATE: 04-14-2020
REVISED DATE: 02-24-2021

XXXVIII. PURPOSE:

A. To establish a policy regarding use of social media and social networking by sworn and unsworn members of the Philadelphia Office of the Sheriff.

B. The Office of the Sheriff endorses the secure use of social media as described below to enhance community engagement, communication, collaboration, and information exchange; streamline processes; and to foster productivity. This policy establishes this agency’s position on the utility and management of social media and provides guidance on its management, administration, and oversight.

C. In so doing, this policy sets forth expectations of Sheriff’s Office employees with respect to their use of social media and social networking, and the direct effect such use has upon the reputation, perception and interests of the Office of the Sheriff and its employees.

D. As advances in technology are constantly emerging, this policy is intended to address social media in general, rather than singular form or mode of social media or networking.

E. The Office of the Sheriff PIO and Chief of Staff will oversee all PSO social media accounts.

XXXIX. BACKGROUND:

A. Social media provides a contemporary and potentially valuable means of assisting the PSO and its personnel in meeting several Sheriff’s Office strategies, including, but not
limited to, community outreach, problem-solving, investigations and crime prevention. Social media also plays a significant role in the personal lives of numerous Sheriff’s Office employees. However, it must be formally and universally recognized that the personal use of social media has the potential to impact the Office as a whole, as well as individual members serving in their official capacity. As such, this policy provides information of a precautionary nature as well as prohibitions on the use of social media by PSO personnel.

B. Social media refers to digital communication platforms that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites, micro-blogging sites, photo and video sharing sites, wikis, blogs, and news sites. Some examples of social media include Facebook, Twitter, Instagram, YouTube, Reddit, and Tumblr.

C. As members of the Office of the Sheriff, employees are embodiments of its mission, values, and guiding principles. It is, thus, essential that each member accept their role as an ambassador of the Office. In doing so, each member must strive to maintain public trust and confidence, not only in his or her professional capacity, but also in his or her personal and on-line activities. Moreover, as members of law enforcement, all sworn members are necessarily held to a higher standard of behavior than general members of the public, the on-line activities of employees of this Office shall reflect such professional expectations and standards.

D. These policies address the use of social media in general and not one particular form.

**XL. DEFINITIONS:**

A. For the purpose of this policy, the following definitions apply:

1. **Social Media:** On-line sources that allow people to communicate, share, and/or exchange information with others via some form of on-line or cellular network platform. Information may include, but is not limited to, text, photographs, video, audio, and other multimedia files.

2. **Social Networking:** Involves using such Internet or mobile formats as Myspace, Facebook, Twitter, Twitch, LinkedIn, Foursquare, Usenet groups, message or on-line bulletin boards, blogs and other similarly developed formats, to communicate with others using the same groups while also networking with other users based upon similar interests, geographical location, skills, occupation, ideology, beliefs, etc.

3. **Internet:** A computer network consisting of a worldwide network of computer networks that use the TCP / IP network protocols to facilitate data transmission and exchange.
4. **Post** (noun): An item inserted into a blog, or an entry to any type of computerized bulletin board, forum, or social media site.

5. **Post** (verb): The act of creating, uploading, editing, or adding to any social media outlet. This includes text, photographs, audio, video, or any other multimedia file.

6. **Blog**: A series of entries, written by either one person or a group of people, in an online journal, usually posted in chronological order, like a diary. Blogs can allow or disallow comments on entries.

7. **Comments**: Responses to a blog post, news article, social media entry or other social networking post.

**XLI. POLICY:**

A. It is the policy of the Office of the Sheriff that all existing laws, rules, regulations, and directives that govern on- and off-duty conduct are applicable to conduct associated with social media and networking.

B. The PSO will clearly identify its Official Social Media Accounts.

1. Where possible, PSO social media accounts shall prominently display the following information and/or statements:
   
   a. PSO contact information and a link to the PSO website.
   b. That pages are maintained by the PSO.
   c. The purpose and scope of the PSO’s presence on the websites.
   d. That the opinions expressed by visitors to the pages do not reflect the opinions of the PSO.
   e. That posted comments will be monitored and that the PSO reserves the right to remove comments at its discretion such as obscenities, off-topic comments, personal attacks, any comments that jeopardize an ongoing investigation or prosecution, or that otherwise impair the PSO’s ability to provide effective law enforcement services to the community.
   f. That any content posted or submitted for posting is subject to public disclosure.

C. Employees May Use Non-Official Social Media Accounts for Investigations.

   a. Any employees using non-official social media accounts for investigative purposes will obtain written permission from the Sheriff, regardless of duty assignment.
   b. These employees will maintain a log of all social media postings to non-official accounts.
D. Social Media Content is Subject to Information Technology and Records Management Laws and Policies.

1. The City of Philadelphia of Information Technology stores and retains content from official PSO social media accounts in compliance with open records laws and policies.

E. When engaging in social networking, employees will strictly adhere to any and all of the following:

1. Existing federal, state, and local laws.


3. Laws regarding public information on arrests, investigations, and personnel data.

F. Employees are prohibited from using their status as members of the Office of the Sheriff to endorse any product or service without prior written permission from the Sheriff or his/her designee.

G. Employees are prohibited from posting images of law enforcement personnel working in an undercover capacity or identifying such personnel as law enforcement officers.

H. Employees are prohibited from using City of Philadelphia or Office of the Sheriff property (on or off-duty) to engage in the personal use of social media.

1. For the purpose of this policy, City and Sheriff’s Office property includes, but is not limited to, desk-top computers, lap-top computers, cell phones, hand-held digital or electronic devices (e.g., iPhones, iPads, Android tablets, Android phones, Blackberry phones, laptops, etc.), and digital storage media.

I. While in on-duty status, employees are prohibited from using privately-owned property to engage in personal use of social media.

J. Employees who are off-duty and using privately-owned property to engage in the personal use of social media, do not represent the City of Philadelphia, the Philadelphia Office of the Sheriff, or any official position maintained by either entity. Under such conditions, employees represent only themselves and their personal interests.

1. This policy covers employee personal use of social media affecting the workplace and/or the PDO ability to perform its public mission,
2. The Office recognizes the role that social media plays in the personal lives of some Department employees. However, the personal use of social media can have bearing on employees in their official capacity as they are held to a high standard by the community.

3. Engaging in prohibited speech outlined in this policy may provide grounds for discipline and may be used to undermine or impeach an officer’s testimony in legal proceedings.

K. There is no reasonable expectation of privacy when engaging in social networking online. As such, the content of social networking websites may be obtained for use in criminal trials, civil proceedings, and PSO investigations.

L. Employees may express themselves as private citizens on social media sites as long as employees do not:

1. Make, share, or comment in support of any posting that includes harassment, threats of violence, or similar conduct.

2. Make, share, or comment in support of any posting that ridicules, maligns, disparages, expresses bias, or disrespect toward any race, religion, sex, gender, sexual orientation, nationality, or any other protected class of individuals.

3. Make, share, or comment in support of any posting that suggests that Department personnel are engaged in behavior reasonably considered to be unlawful or reckless toward public safety.

4. Otherwise violate any law or PSO policy.

M. Employees shall make reasonable efforts to remove content appearing on their social media account that violates this policy upon learning of the offensive content. Employees are prohibited from using racial/ethnic slurs, profanity, personal insults; material that is harassing, defamatory, fraudulent, or discriminatory, or other content or communications that would not be acceptable in a City workplace under City or agency policy or practice.

N. Employees are prohibited from displaying sexually explicit and/or pornographic images, cartoons, jokes, messages, or other material that would be considered in violation of the City and Agency policy preventing Sexual Harassment in City Government.

O. Employees shall not post or otherwise disseminate any confidential information they have access to as a result of their employment with the Office of the Sheriff.
P. Employees may not make any statements, appearances, endorsements, or publish materials that could reasonably be considered to represent the views or positions of the Department.

Q. Employees May Not Use Their City Email Address to Register a Personal Account on Social Media.

XLII. GENERAL CATEGORIES OF SOCIAL MEDIA USAGE

A. The Office of the Sheriff recognizes two general categories of social media usage among employees:

1. PSO-Authorized Use of Social Media.

2. Personal Use of Social Media.

B. Office of the Sheriff/PSO/Agency-Authorized Use of Social Media:

1. PSO-authorized use of social media is defined as the employment of such instruments for the specific purpose of assisting the PSO and its personnel in community outreach, problem-solving, investigation, crime prevention, and other PSO-related objectives.

2. In addition to the rules and regulations set forth in Section 4 of this directive, the following provisions shall apply to PSO-authorized use of social media.

   a. Sheriff's Office employees seeking to represent the PSO via social media outlets (III-A, 2.) shall obtain express permission from the Sheriff or his/her designee, prior to engaging in such activity.

   b. Upon obtaining authorization, when engaging in social media networking, employees shall:

      1) Properly identify themselves as a member of the PSO.
      2) In instances whereby proper identification poses a risk to officer safety or may impede the progress of a criminal investigation, employees, with permission from the Sheriff or their designee may exclude PSO membership from their profiles.
      3) At all times, conduct themselves as representatives of the PSO and, accordingly, adhere to all PSO policies and standards of conduct, and observe conventionally accepted protocols and proper decorum.
      4) Observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.
5) Observe and abide by all existing City of Philadelphia information systems policies, including, but not limited to, "Internet Use and Access" and "Electronic Mail and Messaging."

c. When engaging in PSO-authorized social media networking, PSO employees shall not under any circumstances:

1) Make statements about the guilt or innocence of any prisoner, suspect or arrestee, or comments concerning pending prosecutions.
2) Post, transmit, or otherwise disseminate confidential information, including photographs or videos related to PSO training, activities, investigations, or any other work-related assignment, without specific and express written permission from the Sheriff or their designee.
3) Conduct political activities or private business.

C. Personal Use of Social Media:

1. Personal use of social media is defined as engagement or participation in any personal social networking platform, including but not limited to, personally-owned sites, the sites of others (both known and unknown to the employee), news media pages, professional sites unaffiliated with the Office of the Sheriff, or other information exchange forums.

2. In addition to the rules and regulations set forth in Section 4 of this directive, the following provisions shall apply to personal use of social media while off-duty and using privately-owned property.

   a. Employees shall neither express nor imply that they are.

      1) speaking or acting on behalf of the Sheriff’s Office.
      2) representing or presenting the interests of the Sheriff’s Office.

   b. Employees shall not use their rank, title, or position in a manner that would suggest that they are representing the interests or official position of the agency.

   c. Employees shall not post any depiction or illustration of the Official Seal of the City of Philadelphia, or the Philadelphia Office of the Sheriff name, Sheriff badge, logo, patch, or vehicles, so as to give the appearance of an official site of the City of Philadelphia or the Office of the Sheriff.
d. In addition to the above provisions, when engaging in personal use of social media, employees shall not post any text, photograph, audio, video, illustration, or any other multimedia file related to, or depicting, any of the following:

1) Current, past, or pending PSO investigation.
2) Criminal or civil proceeding pertaining to or arising from any matter involving the PSO, including allegations of misconduct.
3) Brandishing of any weaponry (city-owned or privately-owned; actual or simulated), or any contraband (actual or simulated).
4) Brandishing of tactical instruments (both city-owned and privately-owned), including but not limited to firearm, ASP, baton, OC spray, Electronic Control Weapon (ECW), and mechanical restraints.
XLIII. PURPOSE:

A. This policy pertains to the Office’s response to employee alcohol and substance use and to establish a policy to investigate and detect illegal drug/controlled substance usage by members of the Office of the Sheriff (uniformed and civilian). Drug and alcohol abuse have an adverse effect upon a police officer’s ability to execute their duties. The officer’s life, the lives of fellow officers and the lives of the public depend on the officer’s alertness and the ability to make rational decisions with a clear head unaffected by narcotics, controlled substances, or alcohol.

B. Integrity is an essential element in our relationship with the public and this is undermined when officers use drugs illegally, or are intoxicated on duty and thereby, place themselves above the laws they are sworn to uphold.

C. The administration of drug screening tests for cause is a procedure utilized to detect the presence of drugs in the hair and urine of members of the Office suspected of illegal drug/controlled substance usage. To balance the interest and security of the public in having a drug-free Sheriff’s Office against the individual employee’s right to privacy, drug screening tests for cause will be administered when there is reasonable suspicion to believe that a member of the Office (uniformed or civilian) is illegally using drugs/controlled substances.

D. When reasonable suspicion does exist, the member suspected of illegally using drugs/controlled substances MUST provide hair and urine samples when directed. Refusal will result in immediate suspension from duty and subsequent service of charges and specifications.

E. Drug testing shall be a part of the requirements of a routine physical examination.

F. The Sheriff, Chief Deputy, Undersheriff, and all sworn personnel shall be subject to random drug testing.
G. The use of illicit narcotics is indicative of illegal purchase and possession, and the abuse of controlled substances is illegal in certain circumstances.

H. A deputy has the ultimate responsibility and will be held accountable for knowing what substances they are ingesting or absorbing into their body, whether it is supplements from pills, protein shakes, oils, rubs, or any other form of supplement legally available for purchase but prohibited by this directive.

I. Employees are prohibited from reporting for duty with the odor of an alcoholic beverage on their breath or under the influence of any intoxicant.

J. Employees shall not consume any Food or Beverage in any Tavern or in the Lounge Area of any Restaurant Where Intoxicating Liquor is Sold While Wearing any Recognizable Part of the Police Uniform.

K. Employees Shall Not Consume Intoxicating Beverages While Wearing any Recognizable Part of the Office of the Sheriff Uniform.

1. This prohibition does not apply to the following receptions related to a law enforcement funeral.

2. Employees shall not consume any food or beverage in any tavern or in the lounge area of any restaurant where intoxicating liquor is sold while wearing any recognizable part of the Office of the Sheriff Uniform.

XLIV. PROCEDURE:

A. The methods for drug testing will be by urinalysis and/or hair testing. All physical examinations required under 3-F-1 through 6 will include a urinalysis and/or hair testing. However, for applicant drug testing and reasonable suspicion, a urinalysis and hair test will be conducted. A hair and urinalysis test will be conducted on all reinstatements and medical evaluations. Random tests shall include a urinalysis and a hair test based on a percentage to be determined by the Sheriff.

1. Hair samples will be extracted primarily from the scalp. However, in the event that a necessary amount of specimen cannot be extracted, hair samples may be taken from an alternate site on the body, such as the arms or armpits, legs, chest, or other site deemed appropriate by the Internal Affairs Division (IAD) investigator.

2. Mandatory periodic testing will be instituted for all personnel. This testing may occur up to two (2) times per calendar year for all sworn members of the Office of the Sheriff. This includes personnel “detailed in and/or detailed out.” The methods for drug testing will be a urinalysis and/or hair test. The Sheriff will designate the number of personnel that shall be required to submit samples for
both a urinalysis and hair analysis test. The remainder will only be subject to a urinalysis test.

3. Mandatory periodic testing is separate and distinct from all other categories of drug and alcohol testing.

B. Sworn personnel are ordered to provide a urine and/or hair sample as directed for a drug test under the following circumstances:

1. As part of an ordered physical examination, which includes the following:
   
   a. When a deputy’s actions, appearance, or demeanor indicates a reasonable suspicion that they have used drugs illegally or improperly.
   
   b. When an internal investigation reveals a reasonable suspicion that a deputy has used drugs illegally or improperly.

2. As a component of a routine physical examination required under Section F, subsections 1 through 6.

3. As set forth in this Drug Testing Policy and in Random Drug Testing section(s).

4. Deputies recruit promotional drug testing.

C. In all cases, once a deputy has arrived at a medical testing facility (either a City-contracted hospital, or a laboratory), they will:

1. Be under the direct supervision of the testing IAD Supervisor, where appropriate.

2. Will be assigned a test code for identification purposes in order to maintain anonymity and privacy throughout the sampling and testing procedure.

3. Complete the Office of the Sheriff Test Identification Form and other forms required by the Public Health Department and/or contracted laboratory.

4. Wash their hands thoroughly prior to the delivery of a urine and/or hair sample and shall deliver the sample in a quantity required for laboratory testing purposes. This will be done in the presence of a testing IAD Supervisor where appropriate.

5. Sign the required forms, certifying that the sample corresponds with the test code identification assigned to the subject/deputy.
D. Prescription drugs (controlled and non-controlled) are to be administered as per the instructions of the prescribing medical or dental practitioner. It is the responsibility of the deputy to make the prescribing medical or dental practitioner aware of the safety sensitive nature of the deputy’s job-related duties prior to prescribing any medication.

E. Non-prescribed, over the counter medications must only be used in recommended dosage amounts. Deputies must consider possible effects on job performance, both before and during dosing.

F. Should a deputy have questions or concerns regarding prescribed medications and needs an explanation as to potential side effects and/or therapeutic actions for prescribed medications or an explanation of the label instructions on over-the-counter medications, then the deputy should contact their doctor, pharmacist, or Employee Medical Services, 19th Street and Fairmount Avenue for further interpretation and direction.

G. Medical records, reports, and/or receipts received by the Risk Management Office, in the course of normal business duties, which indicate that a deputy had a positive urinalysis and/or hair test shall be considered reasonable suspicion that a subsequent drug test will produce evidence of illegal and/or abusive use of drugs for purposes of Reasonable Suspicion cases. Thus, upon receipt of this information, all procedures, including subsequent urinalysis and hair testing as set forth in Reasonable Suspicion scenarios shall apply.

H. All information or reports submitted to or received by the Office regarding drug testing is considered strictly confidential and the unauthorized dissemination of this information by a member of the Office shall result in disciplinary action, as described in the Disciplinary Code, including possible dismissal.

XLV. DEFINITIONS

A. Reasonable Suspicion--Sufficient facts or information to justify a reasonable belief that a drug test will produce evidence of illegal and/or abusive use of drugs.

B. Routine Physical Examination--A regularly scheduled examination by the Medical Director, Employee Medical Services.

C. Testing Officer--A member of the Internal Affairs Division (IAD), assigned by the Sheriff, with full authority to ensure the validity of the entire drug testing process.

D. Positive Result--A finding which indicates the presence of illegal drugs or controlled substances and/or non-controlled substances in an individual’s urine and/or hair sample obtained by chemical laboratory testing. A result will be considered positive only after the confirmatory test has identified the presence of illegal drugs or
controlled substances in an individual's urine and/or hair test. Cut-off levels will be established for each drug or drug metabolite to indicate what is considered a positive result by the contracted laboratory. These cut-off levels, which are listed in this directive, and will be set at reliable forensic threshold levels consistent with the levels of reasonable analytical accuracy.

1. Testing will be conducted by an IAD supervisor. Testing Officers will receive training in the proper and legal administration of this directive prior to the start of actual testing and shall receive additional training as required.

E. Blood Alcohol Content - (BAC) The concentration of alcohol in the blood. This measurement can be determined utilizing a blood sample but is more commonly measured using a breathalyzer; a device that estimates the blood – alcohol level from a breath sample.

F. Routine Physical Examination – Examination administered by the Office of the Sheriff under the following conditions:

1. Promotional

2. Reinstatement: any leave of absence of separation from the Office of the Sheriff including military leave for more than 15 working days in a consecutive period.

3. Return from extended sick leave, ten (10) or more consecutive calendar days.

4. Return after admission to a medical facility for observation or treatment, or after undergoing a surgical procedure, regardless of duration of the absence. This provision will apply to injuries and/or conditions arising from motor vehicle accidents as well as other causes and will include “same day” and outpatient procedures.

5. A request for medical evaluation from a Deputy Chief or above.

6. Upon a transfer, assignment, or detail to the following units.

   a. The immediate offices of the Sheriff, Chief Deputy, Undersheriff, or the Chief of Staff.
   c. Internal Affairs Division (IAD).
   d. The Warrant Unit or Civil Enforcement
   e. Firearms/Armory Technicians
   f. Training and Education Services Bureau.
   g. Canine Unit
   h. Any sworn Real Estate function or Civil process activity.
   i. Any other special unit as designated by the Sheriff.
j. The City of Philadelphia will conduct a urinalysis drug screening on deputy sheriff applicants as a part of the pre-employment physical examination conducted by the Public Health Department. An Office of the Sheriff IAD supervisor will conduct a hair analysis test on all applicants as part of the background process.

XLVI. ROUTINE PHYSICAL EXAMINATIONS

A. The Internal Affairs Deputy Chief will have a supervisor assigned to perform the following:

1. Supervise all tests.

2. Ensure that all samples are controlled, and procedures are followed.

3. Obtain results of all tests from the laboratory.

B. During routine physical examinations, the IAD Supervisor assigned to monitor employees returning to work per the Medical Evaluation Unit (19th and Fairmount Ave.) will perform the following procedures:

1. Supervise and observe that the collection of the drug test sample is in accordance with Office of the Sheriff policy.

2. Deliver all records pertaining to the drug tests to IAD for processing and storage until the results are received from the contracted laboratory.

3. If the results of the test are positive, forward the information to the Deputy Chief-IAD for appropriate action as previously outlined in this directive.

4. Inform the deputy that they will be placed on administrative duty as a result of the positive laboratory analysis.

XLVII. RANDOM DRUG TESTING

A. Random drug testing shall be conducted according to the same standards as all other previously outlined tests.

B. The Sheriff will designate the number of personnel that shall be required to submit samples for both a urinalysis and hair analysis test. The remainder will only be subject to a urinalysis test.

C. Random drug testing will be conducted seven days a week, on all tours of duty.
D. Testing will be conducted in IAD Headquarters located at 100 S. Broad Street or can be performed at the pertinent district or unit, Employee Medical Services located at 19th Street and Fairmount Avenue.

E. Selection shall be at random, generated by computer at the contracted laboratory. This selection is taken from the personnel database on a monthly basis by the Chief of Staff and provided to the IAD Deputy Chief. Upon request, the Fraternal Order of Police (FOP) will be provided with a copy of the previous month random selection list, at the beginning of each new month.

1. Under this system, it is possible that a member of the Office may be randomly tested more than once a year. This is because the list includes all sworn personnel who are available and on duty at the time of selection.

F. If personnel selected during the monthly period are unavailable due to legitimate reasons they will not be tested.

G. Personnel notified to appear for random drug testing must appear when scheduled with no exceptions and will not be permitted to report off until they have been tested.

H. When a member IAD is selected for a random drug test, it will be the responsibility of the highest-ranking supervisor on-duty in IAD or a member of the Executive Command Staff to ensure the integrity of the test by being present from the point of notification to the collection of the sample.

I. When a member of the Office of the Sheriff suspects that another member (uniformed or civilian) may be illegally using drugs/controlled substances:

1. Immediately notify Internal Affairs Division Captain or on call IAD Supervisor.
   a. Provide rank, name, and applicable command of suspected member.
   b. Obtain a confidential report/case number.

J. The IAD supervisor notified and directed to investigate an allegation of an Office of the Sheriff employee (uniformed or civilian) who may be illegally using drugs/controlled substances will:

1) Determine if REASONABLE SUSPICION has been established indicating illegal drug/controlled substance usage.
   a. **Reasonable Suspicion** - Exists when evidence or information, which appears reliable, is known to the Sheriff’s Office supervisor and is of such weight and persuasiveness as to make the supervisor, based upon his/her judgment and experience, reasonably suspect that a member of the service is illegally using drugs/controlled substances. Reasonable suspicion that a member is illegally
using drugs/controlled substances must be supported by specific articulatable facts from which rational inferences may be drawn.

b. Reasonable suspicion cannot be based upon mere “hunch” or solely upon poor work performance.

2) Prepare INVESTIGATION REPORT and record all observations and other pertinent data, i.e.,

a. Testing for Impairment by the Sergeant or Non-sworn Supervisor

1) Recognizes that an employee may be under the influence of an intoxicant
2) Notifies a lieutenant
3) Orders the employee to submit to any required tests under this procedure
4) Arranges for another sergeant or supervisor to witness the tests
5) The lieutenant may serve as the witness.
6) Administers or directs the administration of the field sobriety and BAC breath tests
7) Documents results of the test on form.
8) Submits form to lieutenant

b. Lieutenant, or Civilian Director:

1) Reviews the form
2) Determines whether to recommend a Fit-For-Duty test.
   i. If BAC is not consistent with behavior observed, or if substances other than alcohol are suspected, follows 5.170–TSK–1 Fit-For-Duty Testing
3) Arranges transportation for the employee directly to home if medical attention is not needed.
4) Advises employee that he or she is on paid administrative leave until further notice.
5) Forwards all original paperwork under confidential cover to the Human Resources Director with copies under confidential cover to the employee's Deputy Chief
   i. If after office hours, verbally notifies the Duty Captain, Unit Deputy Chief or Human Resources Director

c. Undersheriff and HR Director:

1) Reviews the medical reports for Reporting Medications Which Impair Performance.
2) Evaluates the duty status of the employee.
d. Employee

1) Advises the sergeant or supervisor of the use of medication(s) that might impair performance on duty

e. Sergeant or Non-sworn Supervisor

1) Determines whether the employee will be allowed to perform regular duties, be reassigned to limited duty, or be relieved of duty for that shift

3) Forwards info to applicable Deputy Chief who shall consults with the HR Department and Undersheriff before determining the employee's assignment while using medication

4) Confer with the IAD Deputy Chief (or above) if reasonable suspicion has been established that member is illegally using drugs/controlled substances.

5) Contact the Sheriff, Chief Deputy, Undersheriff, and Deputy Chief of the suspected employee, upon completion of investigation to obtain approval for drug screening tests.

   a. If circumstances indicate drug screening samples must be obtained expeditiously, immediately contact the Deputy Chief of Internal Affairs for approval.

   b. If Deputy Chief of Internal Affairs is not available, the Applicable Executive Staff Member (Chief Deputy, Undersheriff, or Chief of Staff) may be contacted for approval.

K. The Deputy Chief of Internal Affairs shall:

1. Approve request for drug screening test ONLY after carefully determining whether the IAD supervisor conducting investigation has established reasonable suspicion.

2. Contact the Deputy Chief of the employee suspected of illegally using drugs/controlled substances and direct that member being tested be placed on modified assignment pending results of test unless other circumstances warrant suspension from duty.

L. The IAD supervisor directed to investigate an allegation of an Office of the Sheriff employee shall then:

1. Conduct/administer the Random Drug Test and make notifications via Everbridge to Executive Command Staff.
2. Advise member suspected of illegal drug/controlled substance usage that refusal to provide hair and urine samples will result in immediate suspension from duty.

3. Personally, notify the Undersheriff that a drug screening test has been ordered, provide all pertinent information, and obtain identity of member notified.

   a. Add an entry into Internal Affairs Records citing “Drug Screening Test-Log” under caption “Undersheriff notified,” and time and date of notification.
   b. Once hair and urine samples are taken, cite the procedure followed, person taking the samples, applicable screening numbers associated with the samples, and enter copies of all reports generated into Internal Affairs Recording Systems.

4. Ensure that sworn personnel shall not be required to undergo a physical as a part of this test except for personnel who attempt to report off after they have been notified to appear. These officers will be escorted by IAD personnel to an appropriate medical facility for an immediate physical examination and drug test.

XLVIII. MISCELLANEOUS

A. A City Physician, specifically a medical doctor employed by the City/County of Philadelphia, may order a drug screening test without securing the prior approval of the Office of the Sheriff. However, when a City Physician orders a test for a member of the Office, he/she suspects of illegal drug/controlled substance usage, the City Physician will confer with the Chief of Staff, or designee.

B. The investigator’s case folder will be sealed to protect the employee’s right to privacy in cases in which the result of the drug screening test does not indicate the presence of an illegal drug/controlled substance. The folder will not be unsealed without the written authorization of the Chief Deputy or the Undersheriff. The case folder will be filed in the Internal Affairs Recording System. Furthermore, any reference to the administration of the drug screening test in the personal folder of the member concerned will be expunged.

C. An investigating supervisor finding controlled substances/contraband, such as drugs or instruments used to administer drugs (e.g., hypodermic syringes/needles, crack pipes, etc.) on or in the vicinity of a member of the service (uniformed or civilian) suspected of illegal drug/controlled substance usage will have such items invoiced on PROPERTY RECEIPT as “Evidence” and comply with the pertinent provisions of directives relating to processing controlled substances.

D. In addition, the investigating supervisor will ensure the following statement is entered in capital letters on the Property Receipt: “NOT TO BE DESTROYED WITHOUT APPROVAL OF THE UNDERSHERIFF OR ABOVE.”
XLIX. DISCIPLINARY ACTION

A. Disciplinary action of dismissal will be taken against a member of the Office of the Sheriff under the following conditions:

1. A urinalysis and/or hair test indicates a positive result as defined in Section III, “D” of this directive.

2. Refusal of a direct order to submit to a drug test by a deputy. This action shall be considered as a cause to suspend the deputy with the intent to dismiss.

3. Any action or attempt by an officer to alter, taint, or impair the validity of a drug test including any adulteration or substitution of a sample.

4. A positive drug test as per Section IV.

B. Disciplinary action up to and including dismissal will be taken against a member of the Office of the Sheriff under the following conditions:

1. Refusal of a direct order to submit to a breathalyzer test by a deputy.

2. The use of a prescription drug (controlled or non-controlled) which was not prescribed for the deputy by a licensed medical practitioner.

3. The abuse and/or illicit use of prescription and/or non-prescription drugs.

4. Any attempt by a deputy to circumvent, delay, or fail to cooperate in the exercise of the drug testing procedures outlined in this directive.

L. SAMPLE HANDLING

A. The testing of urine and hair specimens of personnel will be completed by a qualified medical laboratory selected by the Office of the Sheriff which meets contract specifications which will ensure results that are legally supportable and scientifically accurate.

B. With the delivery of each specimen, the Office will designate to the testing laboratory only certain specific drugs for which the specimen is to be analyzed. The testing laboratory will report findings only as to those specific substances contained in that official request.
C. To ensure optimum accuracy, the tests will be drug specific. The drug abuse screening test will consist of two tests:

1. The initial test of each urine and/or hair sample will employ a methodology different from the secondary confirmation test.

2. The initial test will use an “emit test” and/or a thin-layer chromatography process unless a different process has been approved by the Office. The testing process at the laboratory for the initial analysis will be completed in 24 to 48 hours.

3. The secondary confirmation test of any positive findings on specific drugs selected to be screened in the subject shall be accomplished by the gas liquid chromatography/mass spectrometry method.

4. The initial test procedure for determining the presence of cannabinoids will be immunoassay. Secondary confirmation testing of a positive result for the presence of cannabinoids will be gas chromatography/mass spectrometry.

D. The testing laboratory contracted by the Office to test urine specimens under this directive must continue the uninterrupted chain-of-custody procedure from receipt of specimens to chain-of-control of all specimens. This will help to establish fundamental accountability and reliability of testing from a legal viewpoint at each stage in the handling, testing, and storing of specimens and reporting of the test results.

E. The testing laboratory is subjected to appropriate external proficiency-testing and internal quality assurance procedures for evaluating the performance of its testing process and procedures. These procedures must be in conformance with Pennsylvania law and contract specifications. The testing laboratory will not be allowed to know the identity of the subject tested.

F. Strict confidentiality must be maintained throughout the entire testing and reporting process. Results of the test will be forwarded only to the Commanding Officer, IAD or the person authorized by the Sheriff to receive test results. Test results must be either hand delivered or sent electronically.

LI. RECONFIRMATION TESTING

A. The Office of the Sheriff contracted laboratory for urine specimens is required to store a portion of a positive urine specimen for a period of one year. Deputies who have tested positive for drugs will have the option of a reconfirmation test. The reconfirmation test will be conducted on the split specimen, which will remain sealed at the lab for one (1) year. The lab conducting the reconfirmation test must be
certified by the U. S. Department of Health and Human Services. The Internal Affairs Division maintains a list of certified labs. The Deputy tested will be responsible for all costs including shipping to a certified lab of their choice and the testing of the specimen.

B. From the date that a deputy has been notified that they have had a positive urine test for drugs, the deputy has 30 days to notify in writing the Deputy Chief of IAD, of their request for a reconfirmation test. The deputy must provide the name and address of the lab, and the name of the contact person at the lab. All costs are the responsibility of the employee.

C. A deputy who has a positive hair test can request a reconfirmation test by providing a second hair sample for testing. The subject deputy must provide the second hair sample within ten (10) days of his notification of a positive test result. The request must be in writing to the Deputy Chief of IAD. The reconfirmation test sample will be sent to the Office of the Sheriff contracted laboratory. All costs of testing are the responsibility of the officer requesting the test.

D. The laboratory conducting the reconfirmation test must provide the Office of the Sheriff Internal Affairs Division with a written report of the results of the testing conducted on behalf of the officer.

LII. DRUG TESTING CUT-OFF LEVELS

A. These listings represent the screening and confirmatory test cut-off levels of the Office of the Sheriff. The Office of the Sheriff may change the test cut-off levels, and add or delete drugs to be screened, as changes in technology or other considerations warrant identification of these, or other substances at other concentrations. The Office will provide notification of any change in test cut-off levels.

B. Cut-off levels (urine) Emit screen GC/MS screen

1. THC/Marijuana Metabolites 20 NG/ML 15 NG/ML
2. Cocaine/Metabolites 300 NG/ML 150 NG/ML
3. Opiates/Metabolites 2000 NG/ML 2000 NG/ML
4. Phencyclidine 25 NG/ML 25 NG/ML
5. Amphetamine/Methamphetamine 500 NG/ML 500 NG/ML
6. Barbiturate 300 NG/ML 300 NG/ML
7. Benzodiazepine/Metabolites 300 NG/ML 300 NG/ML
8. Methaqualone 300 NG/ML 300 NG/ML
9. Methadone 300 NG/ML 300 NG/ML
10. d-Propoxyphene 300 NG/ML 300 NG/ML
11. MDMA 500 NG/ML 500 NG/ML
12. Cut-off levels (hair) Screening GC/MS Reconfirmation Test
13. Cocaine 5ng/10mg 5ng/10mg Limit of Detection
14. Opiates 3ng/10mg 3ng/10mg Limit of Detection
15. PCP 3ng/10mg 3ng/10mg Limit of Detection
16. Amphetamine 5ng/10mg 5ng/10mg Limit of Detection Marijuana 0.01ng/10mg 0.003ng/10mg Limit of Detection

a. All reconfirmation tests for hair and urine will be a limit of detection test.
b. Limit of detection is defined as the lowest concentration at which the laboratory can identify a substance.

C. Since the controlled substances listed above were not meant to be all inclusive of the drugs subject to abuse, the Office reserves the right (e.g., in reasonable suspicion/cause) to perform analysis for additional controlled substances (e.g., steroids). Appropriate forensic analytical techniques, (e.g., gas chromatography/mass spectrometry), will be used to detect, identify and measure (to the limit of quantization) such illicit agents or prescription-only medications.

D. Cut-off levels for drugs not listed above will be at the limit of quantization.

LIII. EXPOSURE TO ILLEGAL CONTROLLED SUBSTANCE

A. Procedure

1. Deputy’s in on-duty or off-duty status who become aware that they indirectly or accidentally have breathed, ingested, (including undercover “forced ingestions”) or otherwise internalized illegal controlled substances, will report such occurrences, take law enforcement action where appropriate, or explain why law enforcement action could not have been taken.

2. The deputy, whether indirectly or accidentally exposed to controlled substance, will immediately submit a memorandum detailing the incident to his/her Deputy Chief. The applicable Deputy Chief will immediately notify the Deputy Chief of Internal Affairs of the incident, retain the original copy of the memorandum in a divisional file, and submit a copy of the deputy’s memorandum to the Deputy Chief of Internal Affairs Unit.

LIV. INTOXICATION

A. When a member is on duty or is off duty but has taken some official law enforcement action and is suspected by law enforcement personnel of being intoxicated or otherwise impaired, the below guidelines will be followed. (See procedure in Part 6 for suspicion of being under the influence of drugs).

1. Responsibilities of the On-Duty Lieutenant or in his or her absence the Sergeant are as follows:
a. Immediately notify Internal Affairs and the member’s Deputy Chief. During non-business hours, the Duty IAD Supervisor will be notified.
b. Relieve the suspected member of any weapons.
c. Prohibit the member from drinking, eating, ingesting, chewing gum or otherwise using any substance until examined by the Philadelphia Police Department Accident Investigation District and receives a breathalyzer exam.
d. Off-duty members who have taken some official law enforcement actions and are suspected of being intoxicated or otherwise impaired shall be deemed on-duty until officially declared off-duty by the Deputy Chief, IAD or higher.
e. If the incident occurs in Philadelphia, obtain copies of the PPD-Intoxication Report Form (82-S-55) from the District Operations Room Supervisor (ORS) for the IAD Supervisor.

2. The responding IAD Supervisor will:

a. Take custody of any weapons retained by the On-duty Lieutenant/Sergeant
b. Prohibit the member from drinking, eating, ingesting, or otherwise using any substance until examined by the Accident Investigation District and receives a breathalyzer exam.
c. Ensure that the Accident Investigation District (AID) Supervisor is notified that an Office of the Sheriff member is being sent for a breathalyzer examination within sixty (60) minutes.
d. If the official law enforcement action taken resulted in serious bodily injury or death, PPD-Homicide will be updated.
e. The responding IAD supervisor must be on location and observe the breathalyzer examination with an AID Supervisor who will verify the results.
f. Ensure the member was transported without delay to the Accident Investigation District for the breathalyzer examination.
g. Detail via memorandum to the Sheriff and Chief Deputy why any examination was conducted after sixty (60) minutes from the time of the initial suspicion, detailing the facts and circumstances for the delay.
h. Obtain a radio time check on “J” Band (1) upon arrival on location, (2) when transportation has commenced, (3) upon arrival at the Accident Investigation District.
i. Notify the member’s Deputy Chief, and deliver any weapons retained from the suspected member.

3. Internal Affairs shall be responsible to review all actions taken pursuant to this section by police personnel for compliance with Office of the Sheriff policy.

B. To refute allegations, when a member is on-duty or is off-duty but has taken some official law enforcement action and is accused, on scene, of being intoxicated or otherwise impaired by a civilian complainant or witness the highest-ranking supervisor responding to the location shall:
1. Conduct an independent examination of the accused member to determine if suspicion exists that the member may be intoxicated or otherwise impaired and document the results either positive or negative on an Office of the Sheriff Incident Report.

   a. If suspicion exists that the member is intoxicated or otherwise impaired, the provisions of Section A shall apply.
   b. If no suspicion exists that the member is intoxicated or otherwise impaired, no further action according to this Directive is needed.

C. If a breathalyzer examination reveals that a member on-duty, reporting on or off duty has any blood alcohol content (BAC) level, or a member off-duty, who has taken some official law enforcement action, has imbibed enough alcohol such that the member is rendered impaired or incapable of safely taking police action

1. Responsibilities of the Commanding Officer of the District of Occurrence or the Duty Captain-Command Inspections Bureau during non-business hours, are as follows:

   a. Retain the member’s weapon or relieve the member of any weapons if initially transported based on civilian accusations.
   b. Ensure the member is transported home and have him or her report for duty on his or her next scheduled working day.
   c. Notify the member’s Deputy Chief, of all actions taken and deliver any weapons retained from the suspected member.

2. For purposes of this section “impaired or incapable of safely taking “law enforcement action” shall be inferred after a member had imbibed a sufficient amount of alcohol such that the alcohol concentration in the member’s breath is .04% or greater within two (2) hours after the member has taken official law enforcement action.

3. The Responsibilities of the member’s Deputy Chief are as follows:

   a. If applicable, ensure the member is suspended for the day Online or via timesheet and type or write “Impaired-Unable to perform duties” in the comments section.
   b. Contact the Employee Assistance Program (EAP) and provide the member’s name and payroll number. Ensure the member is scheduled to meet with a representative of EAP within three (3) calendar days.
   c. Submit a complete and thorough investigation to the Undersheriff for disciplinary charging. This shall include a cover memorandum requesting disciplinary action that must be attached to the package.
d. Safeguard any weapons received and return to members when appropriate.

D. If a member refuses to be transported to the Accident Investigation District and/or refuses to undergo the breathalyzer examination.

1. The responsibilities of the Duty Lieutenant or IAD supervisor, during non-business hours, are as follows:

   a. Give the member a direct order to accompany the designated supervisor to the Accident Investigation District and/or submit to a breathalyzer examination.
   b. If the suspected or accused member is a ranking officer, the next highest rank will be contacted, without unnecessary delay, through the chain of command to issue the direct order identified in Section D-1-a either personally or via telephone.
   c. During non-business hours the Deputy Chief of Internal Affairs or Chief Deputy will be contacted, and the appropriate rank will issue the order.
   d. Notify “J” band and obtain a time check at the time of the member’s refusal to comply with a direct order.
   e. Retain the member’s weapon or relieve the member of any city issued weapons if initially transported based on civilian accusations.
   f. Ensure the member is transported home and have him or her report for duty on his or her next scheduled working day.
   g. Notify the member’s Deputy Chief of all actions taken.

2. The Responsibilities of the member’s Deputy Chief are as follows:

   a. If applicable, ensure the member is suspended for the day on a time sheet or online writing or typing “Impaired-Unable to perform duties-refused direct order” in the comment section.
   b. Submit a complete and thorough investigation to the Undersheriff. A cover memorandum requesting disciplinary action will be attached to the package.

LV. STEROID TESTING

A. Steroids, which are listed as Schedule 3 drugs under the Controlled Substances Act, are legally available only with a prescription. The use of steroids for non-medical purposes is illegal. Non-medical usage of steroids could produce adverse psychoactive effects resulting in on-the-job safety related issues involving the deputy’s own welfare and the welfare of others and is prohibited.

B. The Controlled Substances Act (CSA) defines anabolic steroids as any drug or hormonal substance chemically and pharmacologically related to testosterone (other than estrogen, progestin, and corticosteroids) that promotes muscle growth. Pharmacologically and toxicologically, anabolic steroids act as synthetic testosterone.
For some individuals, the use of anabolic steroids may be associated with psychotic reactions, manic episodes, feelings of anger and hostility, aggression, and violent behavior.

C. Any and all anabolic androgenic steroids, covered by Schedule 3 of the Code of Federal Regulations’ Schedule of Controlled Substances, as amended from time to time, shall be considered steroids. Synthetic and/or metabolic anabolic androgenic steroids that are not covered by Schedule 3, and are not medically prescribed, shall also be considered steroids for the purpose of this directive. The following is a non-exhaustive list of substances that shall be considered steroids under departmental policy:

1. Androstanediol
2. Androstenedione
3. Androstenediol
4. Androstenedione
5. Bolasterone
6. Boldenone
7. Calusterone
8. Clostebol
9. Dehydrochloromethyltestosterone
10. Desoxyn-methyltestosterone
11. 1-dihydrotestosterone
12. 4-dihydrotestosterone
13. Drostanolone
14. Ethylestrenol
15. Fluoxymesterone
16. Formebolone
17. Furazabol
18. 13a-ethyl-17a-hydroxygon-4-en-3-one
19. 4-hydroxtestosterone
20. 4-hydroxy-19-nortestosterone
21. Mestanolone
22. Mesterolone
23. Methandienone
24. Methandriol
25. Methenolone
26. Methyltestosterone
27. Mibolerone
28. 17-a-methyl-^1-dihydrotestosterone
29. Nandrolone
30. Norandrostenediol
31. Norandrostenedione
32. Norbolethone
33. Norclostebol
34. Norethandrolone
35. Oxandrolone  
36. Oxymesterone  
37. Oxymetholone  
38. Stanozolol  
39. Stenbolone  
40. Testolactone  
41. Testosterone  
42. Tetrahydrogestrinone  
43. Trenbolone  
44. Any salt, ester, or ester of a drug or substance listed above; and  
45. Human Growth Hormone

D. Steroid testing will be done on a “reasonable suspicion” basis. The method of testing will be urinalysis. The collection process will consist of two separate test kits being prepared, both of which are derived from an original urine sample. The first test kit will be forwarded to the departments contracted laboratory and will undergo testing for the department’s standard urinalysis drug panel. The second test kit will be tested for steroids. It will also be forwarded to the departments contracted laboratory. If steroid analysis cannot be performed there, the department’s contracted laboratory will forward the in-tact test kit to a laboratory certified by the US Department of Health and Human Services or approved by WADA (World Anti-Doping Agency).

E. The testing laboratory will utilize confirmation testing via gas chromatography / mass spectrometry (GC/MS) and/or liquid chromatography / mass spectrometry (LC/MS) providing the necessary quantum of proof for identifying the presence of the anabolic steroid. Qualitative testing is utilized with the ability to accurately identify the anabolic steroid to the laboratory’s limit of quantification (LOQ) which is typically 1 ng/mL. Testosterone and epitestosterone which are all present in very small quantities in the human body will have cutoff parameters applied as follows:

1. Testosterone and/or epitestosterone, and/or a T/E ratio greater than or equal to 6.0: POSITIVE.
2. Nandrolone which is not normally present in the human body can be present in rare circumstances in very minute quantities; therefore, Nandrolone, or 19-Norandrosterone, or 19-Noretiocholanolone greater than or equal to 10 ng/mL: POSITIVE
3. The presence via confirmation testing of any other anabolic steroid and/or HGH (human growth hormone) as defined in E (3) will be reported positive.

F. If a deputy tests positive for a steroidal type substance and cannot produce evidence of a legitimate prescription for a medically necessary condition, then disciplinary action up to and including dismissal will be incurred. Hence, absent a valid medical reason and/or prescription, the officer will be held accountable for the intake of that particular substance.
G. A deputy who tests positive for a steroidal type substance has the option for a reconfirmation test. From the date that the officer was notified that they had a positive test result, the officer has 30 days to notify in writing the Commanding Officer, IAD, of their request for a reconfirmation test. The reconfirmation test will be conducted on the split specimen, which will remain sealed at the testing laboratory for one (1) year. The laboratory conducting the reconfirmation test must be certified by the US Department of Health and Human Services or approved by WADA (World Anti-Doping Agency). The Officer will be responsible for all costs associated with reconfirmation test.

H. Dietary Supplements

1. Dietary supplements are legal products that are available over the counter in health stores, drug stores, supermarkets, other chain stores and through direct selling companies, physicians, and direct mail catalogs and the internet. When selecting supplements, officers should choose wisely from companies and sources they know as trustworthy.

2. A deputy has the ultimate responsibility and will be held accountable for knowing what substances they are ingesting or absorbing into their body, whether it is supplements from pills, protein shakes, oils, rubs, or any other form of supplement. Warning labels should be read and adhered to. There are some supplements that when ingested and metabolized, could potentially lead to a positive drug test result. If there are any questions or concerns as to the intake of a product, the deputy should consult with their physician or the City Physician located at 1900 Fairmount Ave. for guidance.

3. If a deputy tests positive for a steroidal type substance and cannot produce evidence of a legitimate prescription for a medically necessary condition, disciplinary action up to and including dismissal shall be incurred. Hence, absent a valid medical reason and/or prescription, the officer will be held accountable for the intake of that substance.

BY ORDER OF:

[Signature]

SHERIFF DATE
DIRECTIVE: #48
SUBJECT: CYBER SECURITY INCIDENT RESPONSE PLAN
ISSUE DATE: 04-08-2020
REVISED DATE: 02-24-2021

LVII. POLICY:

A. It is the policy of the Philadelphia Office of the Sheriff to provide guidance to end-users, executives, managers, and suppliers on all prerequisite internal security procedures specific to Information Technology Security Incident and Resolution. This information is critical to maintaining a secure infrastructure and shall be used to mitigate problems encountered by employees, information technology professionals, executive management, and stakeholders when secure information is placed at-risk.

LVII. PURPOSE:

A. The Office increasingly depends on computer-supported information processing and telecommunications. This dependency will continue to grow as we work to make our business more efficient to meet the needs of an ever growing and diverse set of clients. This document outlines the Process and Procedures that must be followed with regards to Information Technology Security Incidents.

B. The goal of these procedures is to ensure adherence to a standardized management plan that protects computer assets, networks and information systems and the security associated with being the custodian of confidential data.

C. The Office’s Information Technology Assets continue to become more critical to the personal and economic welfare of the Office of the Sheriff. Each employee, manager, executive, stakeholder, consultant, and sub consultant always have a responsibility to maintain information protection. This responsibility also extends to having a management program for “what to do when things go wrong.”
D. Incident management is a program which defines and implements a process that the Office of the Sheriff adopts to promote its own welfare and the security of the public.

LVIII. PLAN:

A. Application

1. Employees, subcontractors, suppliers, consultants, and other stakeholders who have responsibility to respond to a Security Incident must use this document to understand how to perform their job functions with regards to the IT Security and incident process and procedures that are contained in this document. These procedures must be followed with regards to Information Technology Security Incidents.

B. Abbreviations and Definitions: the following is a list of common abbreviations and definitions used in this document:

1. Abbreviations:

   a. SHE  Sheriff
   b. CD    Chief Deputy
   c. CS    Cyber Security
   d. RITM  Responsible Information Technology Team Member
   e. FIRT  Office Incident Response Team
   f. DNS   Domain Name Server
   g. DoS   Denial of Service
   h. FBI   Federal Bureau of Investigation
   i. FTP   File Transfer Protocol
   j. I/D   Intrusion Detection
   k. IDS   Intrusion Detection System
   l. IP    Internet Protocol
   m. ISP   Internet Service Provider
   n. IT    Information Technology

2. Definitions:

   a. Adverse event – An event that indicates or produces an actual or potential negative consequence to The Office IT systems. Includes: attempted or actual system crashes, network packet floods, unauthorized use or disclosure, defacement of a webpage, and execution of malicious code. Documented and verified adverse events are incidents.
b. **Adware** – Any software application, which displays advertising banners while running a program. Adware includes additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on the computer screen. It usually includes code that tracks a user’s personal information and passes it on to third parties without the user’s authorization or knowledge.

c. **Botnet** – A network of compromised machines that can be remotely controlled by an attacker. Due to their immense size (tens of thousands of systems that can be linked together), they pose a severe threat to The Office’s IT infrastructure.

d. **Breach** - Any illegal penetration or unauthorized access to a computer system that causes damage or has the potential to cause damage.

e. **Chain of Custody** - Protection of evidence by each responsible party to ensure against loss, breakage, alteration, or unauthorized handling. Protection also includes properly securing, identifying, and dating evidence.

f. **Compromise** – The unauthorized disclosure, modification, substitution, or use of sensitive information or the successful action to invade system by getting around its security. A computer has been compromised, for example, when a Trojan Horse has been installed.

g. **Compromise of Integrity** – Any unauthorized modification of information or data.

h. **Cyber/Computer Security Incident** – A violation or imminent threat of violation of computer security policies, acceptable uses, or standard computer security policies. It is also any adverse event whereby some aspect of a computer system is compromised such as: loss of data confidentiality; disruption of data integrity; disruption of availability, also known as a denial of service.

i. **Damage** – The unauthorized deliberate or accidental physical or logical modification, destruction or removal of information or data from an IT system.

j. **Denial of Service (DoS)** – An inability to use system resources due to unavailability; for example, when an attacker has disabled a system, a network worm has saturated network bandwidth, an IP address has been flooded with
external messages or the system manager and all other users become locked out of a system.

k. **Event** – Any observable or measurable occurrence in a system or network. Events may include, but are not limited to, a user connecting to a file share, a server receiving a request for a Web page, a user sending electronic mail, and a firewall blocking a connection attempt.

l. **Finding** – An event or occurrence that may cause a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. Findings require IT worker and/or RITM analysis prior to becoming an incident.

m. **Firewall** – A system that controls network traffic between two networks to minimize unauthorized traffic or access. Firewalls can protect networks and systems from exploitation of inherent vulnerabilities. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet.

n. **Harm** – To cause damage, injure, or impair IT systems using electronic methods, which can include intangible things such as identity theft.

o. **Incident Closure or Closeout** – The last phase of incident handling lifecycle during which the IT worker submits the incident for review and comment. Closeout is not final until peer review has been completed and all questions regarding the incident are answered satisfactorily.

p. **Incident (Cyber Security)** – A violation or imminent threat of violation of computer security policies, acceptable use, or standard computer security practices. It is also any adverse event whereby some aspect of a computer system is compromised, such as loss of data confidentiality, disruption of data integrity, disruption, or denial of service. The types of incidents are classified into LOW, MEDIUM, or HIGH levels depending on the severity.

q. **Incident Declaration** – The phase of the incident handling lifecycle during which an Office incident number is assigned, and the responsible IT worker begins its incident handling process. An incident is declared by a FIRT team member that is recognized and documented as being responsible for incident handling.
r. **Incident Handling** - The comprehensive management process of receiving incident indications and warnings from Intrusion Detection Systems (IDS), United States Computer Emergency Response Team (US-CERT), law enforcement or Internet Service Providers (ISP) that an incident has occurred. It includes identifying the actual incident type, verifying the victim or perpetrator’s responsible. It also requires reporting, responding to, mitigating, and closing an Office CS incident.

s. **Incident Notification** – This phase of the incident handling lifecycle involves the formal transmission of declared incident information to the documented incident handling or management personnel in the Office that is experiencing a CS incident.

t. **Incident Oversight** – The process of ongoing review and follow-up of incident status by the FIRT organizations, staff, or assignees to maintain accurate Office incident records on the number of incidents declared open, closed, or cancelled. Office-wide incident oversight is required for record keeping and review of close-out reports, as well as potential compliance with contracts and applicable laws.

u. **Incident Preparation** – This phase of the incident handling lifecycle involves preparing reports and providing continuous status on the incident.

v. **Incident Prevention** – This phase of the incident handling lifecycle involves the review of alerts, warnings, and suspected events from various sources. In addition, it involves continuous system monitoring and review of risk assessments for systems with high CS incident rates.

w. **Incident Reporting** - This phase involves a formal acknowledgement by the FIRT that an incident has occurred and that notification of all personnel responsible for responding to, acting upon, or resolving an incident have been notified. The incident reporting process includes notification of the CD, SHE, The Undersheriff, Law Enforcement and Office Contacts as needed.

x. **Incident Response** – The process of acting upon known identified incidents. The process includes analysis of how the incident occurred and actions to contain the incident, eradicate the cause of the incident, repair the damage, and recover from the incident. This phase includes collection and preparation of a lessons learned report and assistance in the development of an incident report.
y. **Incident Tracking** – The process and requirement for The Office to maintain comprehensive records of all incidents from the time of declaration through closure. The Office is required to track incidents and report the status of those incidents periodically to the CD.

z. **Intrusion** – An unauthorized, inappropriate, or illegal activity by insiders or outsiders that can be considered a penetration of a system.

aa. **Intruder** - A person who is the perpetrator of a computer security incident. Intruders are often referred to as “hackers” or “crackers.” Hackers are highly technical experts who penetrated computer systems; the term cracker refers to the experts with the ability to “crack” computer systems and security barriers. Most of the time “cracker” is used to refer to more notorious intruders and computer criminals. An intruder is a vandal who may be operating from within The Office or attacking from the outside of the enterprise.

bb. **Level of Consequence** - The impact an incident has on an organization. Impact includes loss of data; the cost to The Office or mission area; negative consequences to the Office (e.g. damage to reputation); and the magnitude of damage that must be corrected.

c. **Malicious Code** – Also known as “Malware” (malicious software), is a computer code or program designed to deny, destroy, modify, or impede a system’s configuration, programs, data files, or routines. Malicious code comes in several forms, including viruses and worms.

d. **Misuse** - Unauthorized use of an account, computer or network by an intruder or malicious user (or insider).

e. **Need-to-Know** - The necessity for access to, knowledge of, or possession of classified or other sensitive information in order to carry out officially sanctioned duties. Responsibility for determining whether a person’s duties require possession or access to this information rests upon the individual having current possession (or ownership) of the information involved, and not upon the prospective recipient. This principle is applicable whether the prospective recipient is an individual, a contractor, another Federal agency, or a foreign government.

ff. **Pharming** – An exploit of the Domain Name Server (DNS) that tries to or actually transforms the legitimate host name into another IP address. The “pharmer” sets up a website looking similar to a legitimate site and harvests...
personal information from unsuspecting users. This is also known as “DNS cache poisoning.”

gg. **Phishing** – An exploit that imitates legitimate companies’ e-mails to entice people to reveal sensitive or private information or creates a replica of an existing web page to fool a user into submitting personal, financial or password data.

hh. **Rootkit** – A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker’s activities on the host and permit the attacker to maintain root-level access to the host through covert means.

ii. **Spyware** - Any technology that aids in gathering information about a person or organization without their knowledge. Sometimes this software is called a “spycam” or “tracking software.” Spyware is put on someone’s computer to secretly gather information about the user, agency or company and relay it to advertisers, foreign governments, and other interested parties. Spyware can be installed as part of a virus, worm, or result from installation of a program. Spyware is often installed without the user’s consent as a drive-by download, by clicking on some option of a deceptive pop-up or webpage, adware, or e-mail attachment.

jj. **Threat** – A circumstance, condition, or event with the potential to cause harm to personnel and/or network resources in the form of destruction, disclosure, modification of data, DoS, and/or fraud, waste, and abuse. The most common security threats are to network systems. Network security threats include impersonation, eavesdropping, DoS, packet replay/modification.

kk. **Trojan Horse** – A non-self-replicating program that seems to have a useful purpose, but in reality, has a different malicious purpose.

ll. **The Office** – Any Office staff office, mission area, project or working group responsible for purchasing, installing, and managing IT resources.

mm. **Virus** – A piece of malicious code that attaches itself to another program. It does not run on its own but executes when the host program is run.

nn. **Worm** – A type of malicious code that acts as an independent program and can usually replicate itself without human interaction from one system to another.
C. Overview of the Incident Response Plan

1. An IT security incident, for the purpose of all Office procedures is defined as an event that impacts or has the potential to impact the confidentiality, availability, or integrity of Office of the Sheriff Information Technology Assets. Standards, procedures, and guidelines regarding IT security incident response are included in this document.

2. Specific procedures vary depending on the type of incident, but all procedures include the following steps:

   a. Discovery
   b. Documentation
   c. Notification
   d. Acknowledgment
   e. Containment
   f. Investigation
   g. Resolution
   h. Postmortem Review
   i. Closure

3. In order to coordinate response to and resolution of IT security incidents, the Office established an incident response team (IRT) the Office Incident Response Team (FIRT) is led by the Office Administrator (CD) or their designee. FIRT is composed of IT security staff reporting to the RITM and others as appropriate for the incident. FIRT has the following characteristics and responsibilities:

   a. Has primary authority in response decisions for Office IT security incidents
   b. Coordinates incidents from discovery through resolution and closure
   c. Assesses threats to Office IT resources
   d. Determines vulnerabilities of Office IT resources
   e. Processes IT security complaints or incidents reported by others
   f. Alerts Office IT workers of active threats.

4. The following list describes responsibility for each step in the typical incident response process:

   a. FIRT maintains systems to discover security incidents involving Office IT resources
   b. FIRT documents IT security incidents in a tracking system
   c. FIRT sends notifications to IT and department employees identifying the type of incident
   d. Department and IT workers must acknowledge the notification
e. All employees, IT employees and FIRT members must focus on containing the incident as soon as possible
f. FIRT must investigate and update the tracking system with details of the investigation
g. FIRT, using details from the investigation, determines incident severity
h. Units must update the tracking system when the incident is resolved
i. FIRT reviews incidents in the tracking system and closes tickets as appropriate

5. FIRT can be contacted with any questions regarding incident response. Office contractors, subcontractors and consultants should form and prepare incident response teams in their companies. Office contractors, subcontractors and consultant response teams are led by the local IT Manager or their designee and composed of contractors, subcontractors, and consultant IT workers. Office contractors, subcontractors and consultant must respond to and resolve all incidents reported to them. They must report to FIRT all incidents discovered in their organization that either has or has the potential to cause loss of Office Confidential Data.

6. Incidents include one or more of the following:

a. Suspected computer or network break-in (of an Office computer or by Office computer).
b. Firm website defacements or compromises, including failure to take the website offline or deregister the URL when the website is no longer used or supported by The Firm.
c. Successful DOS attacks by Office computers or against Office computers.
d. Computer Virus/Worms/Trojan Horses for which anti-virus software updates are not available or their deployment will be delayed (depending on impact to Firm/Department/Location).
e. Detection of malware, including viruses, worms, Trojan Horses, or spyware, caused by employees who have declined to bring laptops into the office for upgrades.
f. Connection of non-Firm computers and servers to the Office network without authorization or in violation of security policies.
g. Unauthorized use of a system for processing or storing non-Firm or prohibited data or information on Office IT resources, including the establishment and operation of a private or personal business.
h. Changes to system hardware, firmware, or software without the system owner’s authorization.
i. Property destruction related to a CS incident (exceeding $100,000).
j. Personal theft related to a CS incident (exceeding $100,000).
k. Electronic file transfer (EFT) exploitation/manipulation or engaging in Phishing or Pharming.

324
l. Installation use or sharing of Peer-To-Peer Software.
m. Activity including unauthorized or illegal serving out, downloading or sale of copyright material.

n. Child pornography.
o. Pornography.
p. On-Line gambling.
q. Attempts to circumvent access to any Office blocked Web Sites such as pornography, gambling and hate crimes.

r. Download use or sharing of copyright protection music or unauthorized software.
s. Misuse of Office property, facilities or services including accepting payment or services to provide access to or use of Office IT resources in excess of one’s authority, such as forwarding spam, engaging in unofficial/unauthorized chat, non-Firm e-mail and instant messaging services; and

t. Any violation of law.
u. Adverse action resulting in employee termination in which the Office computer is neither the tool nor target of the action.
v. US-CERT priority level 3 activity.
w. IDS reports that define activity as medium.
x. Unauthorized use of a system for processing or storing Office data.
y. Property destruction related to a CS incident (less than $100,000).
z. Personal theft related to a CS incident (less than $100,000).

aa. Misuse of Office property, facilities, and services.
bb. Unconfirmed computer virus/worms (depending on impact to Enterprise/Department and if the infection is the result of a security policy violation); and

cc. Undocumented or unapproved vulnerability scans.

dd. Loss or compromise of a personal password.

ee. Suspected sharing of Office accounts.

ff. Minor misuse of Office property, facilities, and services.


hh. Unsuccessful scans/probes (internal & external); and

ii. Computer virus/worms (depending on impact to Enterprise/Department).

D. Incident Response Procedures

1. Incident Response Procedures for Vulnerabilities

a. Examples: patch or upgrade needed, weak password, unrestricted access:

1) Discovery: The Office Incident Response Team (FIRT) assesses threats to Office IT resources. When a threat is discovered, it is documented, and IT workers are alerted. When possible, Office IT resources are assessed for vulnerability to the newly discovered threat and appropriate contacts are
notified. FIRT continuously scans Office address space for vulnerabilities of concern using an industry standard vulnerability scanner. IT workers must vet security lists, web sites and other resources for patches to vulnerabilities in software for which they are responsible.

2) Documentation: FIRT tracks discovered vulnerabilities in a tracking system.

3) Notification: When a vulnerability is discovered by the Office Incident Response Team, appropriate contacts are notified via email. The recipient list of FIRT notifications may be augmented as needed to include staff with appropriate knowledge and skills. Key FIRT Contact Information is listed in Attachment A.A “Key FIRT Contact Information”

4) Acknowledgment: Not all vulnerability notifications require acknowledgment; follow the instructions included with the notification. For accurate tracking of vulnerabilities and to avoid erroneous notifications, false positives should be reported using the URL included with the notification.

5) Containment: IT resources with vulnerabilities should be contained until the vulnerability is resolved.

6) Investigation: Network and server managers must investigate vulnerabilities identified in notifications. IT workers must research applicable security resources to determine the appropriate remediation.

7) Resolution: Network and server managers must resolve vulnerabilities identified in notifications. IT workers should follow unit change management procedures to make software updates. Common resolutions to correct vulnerability include upgrading and patching. Alternatives include physical, network, host, user and/or other access restrictions. Other resolutions may also apply.

8) Postmortem Review. Prior to closing any ticket regarding an incident, FIRT must conduct a postmortem review for the purpose of the following:

a. Identify the root cause of the incident and
b. Identify the steps that need to be taken to reduce the likelihood of a repeat of this type of incident and
c. Document the operational changes that need to take place to prevent a recurrence of the incident and
d. Implement the new operational changes
9) Closure. FIRT reviews the tracking system and closes tickets when appropriate. FIRT has primary authority in response decisions for Office IT security incidents and coordinates incidents from discovery through resolution and closure. FIRT can be contacted with any questions regarding incident response.

LIX. INCIDENT RESPONSE PROCEDURES FOR COMPROMISED RESOURCES

A. Examples: attack/exploit, backdoor or trojan, denial of service, virus, malware, unauthorized access.

1. Discovery. FIRT receives and processes discovery notifications from other sources. FIRT manages systems to discover compromised IT resources on the Office network. FIRT must also deploy systems to detect compromised IT assets within laptops, workstations and other devices as needed. Employees must notify FIRT of potential or perceived compromises discovered in their department and on their device.

2. Documentation. The FIRT documents incidents of compromised IT resources in a tracking system. The tracking system retains a detailed log, including accurate times, maintained during the incident. The immediate IT worker responsible for resolution prepares a summary of the incident for:
   a. the Office Administrator (FA),
   b. attachment to the ticket
   c. affected Data Principals and
   d. other relevant management.

3. The following information should be included in the summary:
   a. How the incident was detected
   b. Dates
      1) Inferred date of compromise
      2) Date the compromise was detected
      3) Date the incident was contained
      4) Date the incident was finally resolved
   c. Names
      1) People added to the Office Incident Response Team (FIRT) for this incident
      2) Person responsible for the IT Resource
      3) Person compromising the resource, if known

327
d. Investigation and scope

1) Cause of the compromise
2) Impact of the incident
3) Incident severity

c. Nature of the resolution

d. Proposed improvements

4. This summary for management will probably contain sensitive information and in any case would not be targeted at the user community. Where appropriate, the IT Worker assigned to the ticket should also prepare an incident summary for the users, using the incident as an object lesson to reinforce safe practices.

5. Notification: Contacts for compromises detected by FIRT are identified as Attachment A, "Key FIRT Contact Information." The recipient list of FIRT notifications may be augmented as needed to include staff with appropriate knowledge and skills. Appropriate contacts are notified and recorded in the tracking system. The Department Head will be copied on all notifications. Follow the URL in the notification to a web form that is to be used for entering updates about the incident. If no URL is provided, contacts must respond to the original notification, including content of the original notification, to acknowledge receipt, containment, and commencement of the investigation. If any incident involves unauthorized disclosure or acquisition of private data, the IT worker assigned to the ticket must immediately notify the Office Administrator (FA), Office Privacy Officer / IT Director and his designee. The CD will direct notification to the Office Executive Team, law enforcement and other parties as appropriate. The CD must notify the Senior Attorney Partner of any incident that impacts mission critical service at the enterprise level. Law enforcement should be notified immediately of incidents involving threat to persons or property. The Undersheriff or his designee should be consulted regarding other incidents before contacting law enforcement. The CD and SHE must consult with the Undersheriff and other parties as needed to determine if law enforcement should be notified. When incidents involve law enforcement, contact the Local Police Department the Undersheriff and/or the District Attorney as appropriate. The CD and SHE must also determine if need to notify the Office Client based on the specific contract terms for each client and extent of the lapse. IT workers do not make disciplinary decisions unless they are the supervisor of the violator. If the incident involves an employee, notify the FA, Director or Department Head. In all events, follow Office disciplinary procedures defined by the Office Employee Handbook. Office Clients must be notified of any incident likely to draw public interest. FIRT must be notified when any employee, stakeholder, consultant, or sub consultant discovers an incident that poses a potential threat to other IT resources.

6. Acknowledgment: FIRT notifications should be acknowledged immediately.
7. Containment: Office IT resources engaged in active attacks against other IT resources must be contained immediately. Unless further investigation requires unrestricted access, all other compromises must be contained as soon as possible, but no later than the same business day in which the notification is received. Service might be interrupted to hosts involved in compromises that are not contained on the same business day. For special consideration regarding service disruption, critical servers can be registered according to procedures detailed earlier in this document. Containment can be achieved by immediately disconnecting the resource from the network, revoking user access, or other means as appropriate. IT workers may coordinate with the FIRT to restrict access to compromised hosts that can't be immediately disconnected or must remain connected in a restricted environment for the purpose investigation or providing service. FIRT has the authority to coordinate with Office Network Engineers to block compromised services and/or hosts that present a definitive danger to the rest of the network. Notification will follow the procedures outlined in the Service Interruption Notification section above.

8. Investigation: Investigation includes analysis, identification, prioritization, and evidence collection and retention.

a. Analysis: Compromised hosts must be assessed using the following process:

9. For Windows Client Computers

a. Unusual Processes and Services

1) Ensure the systems engineer running these steps are familiar with the normal processes and services on the machine and search for deviations from the norm.
2) Look for unusual/unexpected processes by running Task Manager:
   - Start > Run and type taskmgr.exe
3) On Windows machines, focus on processes with Username “SYSTEM” or “Administrator” (or users in the Administrator’s Group)
4) Look for unusual started network services (GUI):
   - C:\>services.msc

b. Unusual Files and Registry Keys

1) Check file space usage to look for sudden major decreases in free space, using the GUI (right click on partition) or type:
   - C:\>dir c:
2) Look for unusually big files:
   - Start > Search > For Files or Folders . . . Search Options > Size > At Least 10000 KB
3) Look for strange programs referred to in registry keys associated with system startup by running regedit:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx

c. Unusual Network Usage

1) Look at the shares and make sure that each has a defined business purpose
   - C:\> net view \127.0.0.1
2) Look at which sessions this machine has opened with other systems:
   - C:\> net use
3) Look at NetBIOS over TCP/IP activity:
   - C:\> nbstat -S
4) Look for unusual listening TCP and UDP ports
   - C:\> netstat -na
5) For continuously updated and scrolling output of this command every 5 seconds:
   - C:\> netstat -na 5
6) For Windows Clients include the -o flag for showing owning process id:
   - C:\> netstat -nao 5
7) Gain a general understanding of the normal port usage for the system and look for deviations.

d. Unusual Scheduled Tasks

1) On Windows, check locally scheduled tasks using the schtasks command:
   - C:\> schtasks
2) Also check the scheduled tasks using the Task Scheduler GUI, invoked by going to Start > Programs > Accessories > System Tools > Scheduled Tasks
3) Look for unusual scheduled items, especially those that run as a user in the Administrator's group, as SYSTEM, or with a blank username.
4) Look for unexpected entries in user account directories:

   - C:\Document and Settings\[username]\Start Menu\Programs\Startup
   - C:\Winnt\Profiles\[user_name]\Start Menu\Programs\Start Up
   - C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
5) On Windows, check AutoStart items: Start > Run . . . msconfig.exe, look at Startup Tab

e. Unusual Accounts

1) Look for new, unexpected accounts in the Administrators group:
   - C:\>lusrmgr.msc

2) Click on Groups, Double Click on Administrators, then check members of this group

f. Unusual Log Entries

1) To look at logs, run the Windows event viewer:
   - C:\>eventvwr.msc

2) Or, invoke the event viewer by going to
   - Start > Program > Administrator Tools > Event Viewer

3) Look for suspicious events, such as:
   - “Event log service was topped”
   - “Windows File Protection is not active on this system”
   - “The protected System file [file name] was not restored to its original, valid version because the Windows File Protection.”
   - “The MS Telnet Service has started successfully.”
   - Look for large number of failed logons attempts or locked out accounts.

g. Other Unusual Items

1) Look for unusually sluggish performance and a single unusual process hogging the CPU: Task Manager > Process and Performance Tabs

2) Look for unusual system crashes, beyond the normal level for the given system

h. Identification. Identify source as appropriate, including user, host, or other resource.

i. Evidence Collection and Retention.
1) If forensic evidence is needed for law enforcement (see Response Procedures for Incidents Involving Law Enforcement), an image of the compromised host must be retained. Email and any other relevant evidence must also be retained.

2) If the method of compromise is unique or cannot be determined, evidence should be retained to aid in analysis of the incident.

10. For Windows Servers

a. Unusual Processes and Services

1) Look for unusual/unexpected processes, and focus on processes with Username “SYSTEM” and “Administrator” (or users in the Administrators’ group) You need to be familiar with normal processes and services and search for deviations

2) Using the GUI, run Task Manager:
   - C:\> taskmgr.exe

3) Using the command prompt:
   - C:\> tasklist
   - C:\> wmic process list full

4) Also look for unusual services

5) Using the GUI:
   - C:\> services.msc

6) Using the command prompt:
   - C:\> net start
   - C:\> sc query

7) For a list of services associated with each process:
   - C:\> tasklist /svc

b. Unusual Files and Registry Keys

332
1) Check file space usage to look for sudden major decreases in free space, using the GUI (right click on partition) or type:
   - C:\>dir c:\n
2) Look for unusually big files:
   - Start > Search > For Files or Folders ... Search Options > Size > At Least 10000 KB

3) Look for strange programs referred to in registry keys associated with system startup by running regedit:
   - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
   - HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
   - HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx

4) Note that you should also check the HKCU counterparts (replace HKLM with HKCU above)

5) Using the GUI:
   - C:\> regedit

6) Using the command prompt:
   - C:\> req query <reg key>

c. Unusual Network Usage

1) Look at the shares and make sure that each has a defined business purpose
   - C:\> net view \127.0.0.1

2) Look at which sessions this machine has opened with other systems:
   - C:\> net use

3) Look at NetBIOS over TCP/IP activity:
   - C:\> nbstat -S

4) Look for unusual listening TCP and UDP ports
   a. C:\> netstat -na

5) For continuously updated and scrolling output of this command every 5 seconds:
   b. C:\> netstat -na 5

6) For Windows Servers include the -o flag for showing owning process id:
   c. C:\> netstat -nao 5

7) The -b flag shows the executable name and the DLLs loaded for the network connection.
   d. C:\> netstat -naob 5
8) Gain a general understanding of the normal port usage for the system and look for deviations.

d. Unusual Scheduled Tasks

1) Look for unusual scheduled items, especially those that run as a user in the Administrator's group, as SYSTEM, or with a blank username.

2) Using the GUI, run Task Scheduler:
   - Start > Programs > Accessories > System Tools > Scheduled Tasks

3) Using the command prompt
   - C:\>schtasks

4) Check other AutoStart items as well, for unexpected entries, remembering to check user AutoStart directories and registry keys

5) Using the GUI, run msconfig and look at the Start Up tab:
   - Start > Run, msconfig.exe

6) Using the command prompt:
   - C:\> wmic startup list full

e. Unusual Accounts

1) Look for new, unexpected accounts in the Administrators group:
   - C:\>lusrmgr.msc

2) Click on Groups, Double Click on Administrators, then check members of this group

3) This can also be done at the command prompt:
   - C:\>net user
   - C:\>net local group administrators

f. Unusual Log Entries

1) Look for suspicious events, such as:

   - “Event log service was stopped”
   - “Windows File Protection is not active on this system”
   - “The protected System file [file name] was not restored to its original, valid version because the Windows File Protection.”
   - “The MS Telnet Service has started successfully.”
- Look for large number of failed logons attempts or locked out accounts

2) To look at logs, run the Windows event viewer:
   - C:\>eventvwr.msc

3) Using the command prompt

4) Or, invoke the event viewer by going to
   - Start > Program > Administrator Tools > Event Viewer

g. Other Unusual Items

1. Look for unusually sluggish performance and a single unusual process hogging the CPU: Task Manager > Process and Performance Tabs
2. Look for unusual system crashes, beyond the normal level for the given system.
   i. Identification. Identify source as appropriate, including user, host, or other resource.
   ii. Evidence Collection and Retention.

3. If forensic evidence is needed for law enforcement (see Response Procedures for Incidents Involving Law Enforcement), an image of the compromised host must be retained. Email and any other relevant evidence must also be retained.

4. If the method of compromise is unique or cannot be determined, evidence should be retained to aid in analysis of the incident.

B. If the incident involves law enforcement, secure evidence without reviewing additional content. Network hardware, software or data may be considered evidence. Care must be taken to preserve evidence.

C. A public records request, subpoena, warrant or other official request must be issued before data is released to law enforcement. Contact the Undersheriff to review all public records requests, subpoenas, and warrants before responding. Evidence from incidents that involve an immediate threat to persons or property may be provided to law enforcement in advance of a public records request, subpoena, or warrant, but the Undersheriff should be contacted if time allows. FIRT must be informed of incident investigation details. Using the URL provided in the original notification, IT workers should access a web form for entering details about the incident investigation. When saved, this form will automatically notify FIRT and update the tracking system. If no URL is provided, contacts must respond to the original notification, including content of the original notification, to provide details of the
investigation. Using the investigation details provided by IT workers, FIRT classifies incident severity.

1. Resolution. Compromises must be resolved as soon as possible, preferably the day of the notification. Compromised hosts must be reformatted, rebuilt, and have vulnerabilities resolved before reconnecting them to the network. However, at the discretion of the FA, compromised hosts may be cleaned and patched expeditiously.

2. Incidents must be resolved to the satisfaction of the FIRT before compromised hosts are reconnected to the network or filters are lifted. In some cases, the FIRT may request privileged access to ensure the host is safe to resume network connectivity or may require that it be evaluated for vulnerabilities before being placed back in service.

3. FIRT must be informed of incident resolution details. Using the URL provided in the original notification, IT workers should access a web form for entering details about the incident resolution. When saved, this form will automatically notify FIRT and update the tracking system. If no URL is provided, contacts must respond to the original notification, including content of the original notification, to acknowledge the resolution.

4. The incident classification must be entered in the ticket before the status is changed to Resolved. Using the investigation details provided by IT workers, FIRT classifies incident severity.

5. The IT workers responsible for the IT resource that has been compromised must distribute to impacted users and their supervisors a user-oriented summary of the compromise including:

   a. Impact on the user's work
   b. Remediation or preventative measures the users should take

6. In particular, if passwords have been compromised, they must be reset and changed by the users, once the system has been secured.

7. Postmortem Review. Prior to closing any ticket regarding an incident, FIRT must conduct a postmortem review for the purpose of the following:

   a. Identify the root cause of the incident and
   b. Identify the steps that need to be taken to reduce the likelihood of a repeat of this type of incident and
   c. Document the operational changes that need to take place to prevent a recurrence of the incident and
   d. Implement the new operational changes
8. Closure. FIRT reviews the tracking system and closes tickets when appropriate. FIRT has primary authority in response decisions for Office IT security incidents and coordinates incidents from discovery through resolution and closure. FIRT can be contacted with any questions regarding incident response.

D. Incident Response Procedures for Copyright Infringement

1. Examples: unlicensed movies, music, or software.

a. Discovery. Any formal Digital Millennium Copyright Act (DMCA) complaints received directly from a representative of the copyright holder should be referred to The Office's designated agent for DMCA complaints (dmca@thefirm.com). Non-DMCA complaints (complaints not intended to conform to the requirements of the DMCA) should be resolved by the Department Head if possible. If not easily resolved, forward non-DMCA complaints to dmca@thefirm.com. Upon receipt of a complaint, The Office's DMCA agent will examine the notice of copyright infringement to determine whether it contains the elements required by the DMCA.

1) Identification of the copyrighted work claimed to have been infringed.
2) Identification of the material that is claimed to be infringing and that is to be taken down or disabled, and information "reasonably sufficient" to enable the service provider to locate the materials.
3) Information "reasonably sufficient" to enable the service provider to contact the complainant.
4) A physical or electronic signature of a person authorized to act on behalf of the owner (i.e., the copyright owner or its licensee) of the right that is alleged to be infringed.
5) A statement that the complainant has "a good faith belief" that use of the material in the manner complained of is not authorized by the copyright owner, the owner's agent, or the law.
6) A statement that the information in the notification is accurate and that, under penalty of perjury, the complainant is authorized to act on behalf of the copyright owner.

b. Documentation. FIRT documents alleged copyright infringement complaints in a tracking system.

c. Notification. If the notice substantially complies with a, b, and c above, The Office's DMCA agent will forward the complaint to the appropriate IT worker and the Sheriff as listed in Attachment B, "The Office Contact List." If the complaint complies with a, b, and c, but does not substantially comply with d, e, and f, more information may be requested from the complainant. Only if the notice does not adequately comply with a, c, and c above or if the complainant does not respond to request for more information can the Office DMCA agent disregard the notice.
d. Acknowledgment. DMCA notifications must be acknowledged immediately.

e. Containment. The procedures listed below must be followed upon receipt of a notice of copyright violation from the Office DMCA Agent:

1) The CD and/or his designee will ensure that public access to the material targeted by the complaint is disabled as quickly as reasonably possible. If after one business day this action has not been taken, the Office’s DMCA agent will request that Office Information Technology block access to the material.

2) The CD and Sheriff will ensure that the person believed to be responsible for the alleged infringing distribution of copyrighted material is notified of the complaint, and of the action taken to remove access to the material. The person must be given an opportunity to contest the removal of the material if they believe the complainant has misidentified it or if the material is lawful. If they choose to contest the removal, follow the Counter Notification procedures below.

3) If the material in question is not legally possessed by the person believed responsible for making it publicly accessible, the CD and / or Sheriff will ensure that the material is removed from the system on which it was found.

4) The CD will ensure that the Office DMCA agent is notified when the material is no longer publicly accessible, and that the Office DMCA agent is notified if the person responsible for distributing the material is contesting its removal.

f. The Office’s Human Resources Department Head and SHE must be notified of the existence of the DMCA complaint of the name of the party responsible for distributing the e-mail.

g. Investigation. If the person responsible for the alleged infringing distribution of copyrighted material believes the material was misidentified or the distribution was lawful, they should send a counter-notification to the Office DMCA agent. The counter-notification must contain the following:

1) A physical or electronic signature of the person responsible for the alleged infringing distribution.

2) Identification of the material (or the location of the material) to which public access has been disabled. The identification should match the original identification provided by the complainant.

3) A statement under penalty of perjury that the alleged infringer has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material obtained via internal investigation if the violator is a sworn employee.
4) The alleged infringer's name, address and telephone number, and a statement that the alleged infringer consents to the jurisdiction of the federal district court for the judicial district in which the alleged infringer is located and that the alleged infringer will accept service of process from the complainant.

h. Resolution. The Office DMCA agent should work with the alleged infringer to obtain any missing components of the counter-notification. When the counter-notification is complete, the Office DMCA agent will forward it to the complainant, along with a notification that the removed material may be restored in ten business days unless legal action is commenced against the alleged infringer. If the complainant fails to notify the Office DMCA agent that it has initiated legal proceedings within ten business days after receiving a counter-notification, the Office DMCA agent will notify the CD and Sheriff that the material may be returned to public distribution.

i. Postmortem Review. Prior to closing any ticket regarding an incident, FIRT must conduct a postmortem review for the purpose of the following:

1) Identify the root cause of the incident and
2) Identify the steps that need to be taken to reduce the likelihood of a repeat of this type of incident and
3) Document the operational changes that need to take place to prevent a recurrence of the incident and
4) Implement the new operational changes

j. Closure. FIRT reviews DMCA incidents in the tracking system and closes tickets as appropriate. FIRT has primary authority in response decisions for The Office DMCA incidents and coordinates incidents from discovery through resolution and closure. FIRT can be contacted with any questions regarding incident response.

E. Incident Response Procedures for Violations of the Pol-007 Policy on Acceptable use of Company Email, Internet, and Company Assets (AUP)

1. Examples: excessive or disruptive use, complaint, spam, inappropriate content, suspicious activity.

a. Discovery. IT workers that identify violations of the Office Policy on Acceptable use of Company Email, Internet and Company Assets should take action as reasonably necessary to protect The Office and IT resources and notify the violator of the action.

1) Documentation. FIRT documents AUP violations in a tracking system.
2) Notification. Contacts for AUP violations detected by FIRT are identified as Attachment A, "Key FIRT Contact Information." The recipient list of FIRT notifications may be augmented as needed to include staff with appropriate knowledge and skills. Appropriate contacts are notified and recorded in the tracking system. The FIRT notifications may be augmented as needed to include staff with appropriate knowledge and skills. Appropriate contacts are notified and recorded in the tracking system. The Sheriff will be copied on all notifications. Follow the URL in the notification to a web form that is to be used for entering updates about the incident. If no URL is provided, contacts must respond to the original notification, including content of the original notification, to acknowledge receipt, containment, and commencement of the investigation. If any incident involves unauthorized disclosure or acquisition of private data, IT workers and Department Heads must notify the CD who functions as The Office Privacy Officer / IT Director. The privacy officer will direct notification to other executives, law enforcement, Office clients and other parties as appropriate. Law enforcement should be notified immediately of incidents involving threat to persons or property. The Office's Attorney should be consulted regarding other incidents before contacting law enforcement. The FA, IT Engineers and Department Head must consult with the Undersheriff to determine if law enforcement should be notified. When incidents involve law enforcement, contact the Philadelphia Police Department Detective Division and the Undersheriff. IT workers do not make disciplinary decisions unless they supervise the violator. The Sheriff must be notified regarding all incidents involving their direct reports. In all events, follow Internal Affairs investigative policies. The FA, Department Heads and IT Engineers must notify the SHE of any incident likely to draw public interest. The Sheriff must be notified regarding any incident within the Office.

3) Acknowledgment. FIRT notifications should be acknowledged immediately.

4) Containment. AUP violations must be contained immediately. Unless further investigation requires unrestricted access, all other violators must be contained as soon as possible, but no later than the same business day in which the notification is received. Service might be interrupted to violators that are not contained on the same business day. Containment can be achieved by immediately disconnecting the user from the network, revoking user access, or other means as appropriate. IT workers may coordinate with the FIRT to restrict access to violators that can't be immediately disconnected or must remain connected in a restricted environment for the purpose of investigation or providing service. FIRT has the authority to coordinate with resources to block violators that present a danger to the rest of the network.
5) Investigation. If the incident involves law enforcement, secure evidence without reviewing additional content. Network hardware, software or data may be considered evidence. Care must be taken to preserve evidence. A public records request, subpoena, warrant or other official request must be issued before data is released to law enforcement. Contact the Undersheriff to review public records requests, subpoenas, and warrants before responding. Evidence from incidents that involve an immediate threat to persons or property may be provided to the appropriate law enforcement entity in advance of a public records request, subpoena, or warrant, but the Undersheriff will be contacted. FIRT must be informed of incident investigation details. Using the URL provided in the original notification, IT workers should access a web form for entering details about the incident investigation. When saved, this form will automatically notify FIRT and update the tracking system. If no URL is provided, contacts must respond to the original notification, including content of the original notification, to provide details of the investigation. Using the investigation details provided by IT workers, FIRT classifies incident severity.

6) Resolution. FIRT must be informed of incident resolution details. Using the URL provided in the original notification, IT workers should access a web form for entering details about the resolution. When saved, this form will automatically notify FIRT and update the tracking system. If no URL is provided, contacts must respond to the original notification, including content of the original notification, to acknowledge the resolution. The incident classification must be entered in the ticket before the status is changed to Resolved. Using the resolution details provided by IT workers, FIRT classifies incident severity.

7) Postmortem Review. Prior to closing any ticket regarding an incident, FIRT must conduct a postmortem review for the purpose of the following:

   a. Identify the root cause of the incident and
   b. Identify the steps that need to be taken to reduce the likelihood of a repeat of this type of incident and
   c. Document the operational changes that need to take place to prevent a recurrence of the incident and
   d. Implement the new operational changes

8) Closure. FIRT reviews the tracking system and closes tickets as appropriate. FIRT has primary authority in response decisions for The Office IT security incidents and coordinates incidents from discovery through resolution and closure. FIRT can be contacted with any questions regarding incident response.
F. Incident Response Procedures for Suspicious Activity

1. Examples: sweeps, scans, unusual connections, excessive bandwidth consumption

   a. Discovery. FIRT receives and processes discovery notifications from other sources. FIRT manages systems to discover suspicious activity on the Office network. Department Heads must notify FIRT of suspicious activity discovered in their department that has the potential to impact other divisions and the network as a whole. If a deputy chief becomes aware of a suspicious activity in another division, the CD must be notified, and the FIRT and the Sheriff should be copied.

   b. Documentation. FIRT documents suspicious activity in a tracking system.

   c. Notification. When suspicious activity is discovered by the Office Incident Response Team, appropriate contacts are notified. Contacts for suspicious activity detected by FIRT are identified as Attachment A, "Key FIRT Contact Information." The recipient list of FIRT notifications may be augmented as needed to include staff with appropriate knowledge and skills. Appropriate contacts are notified and recorded in the tracking system. The CD and Sheriff will be copied on all notifications. Follow the URL in the notification to a web form that is to be used for entering updates about the suspicious activity. If no URL is provided, contacts must respond to the original notification, including content of the original notification, to acknowledge receipt, containment, and commencement of the investigation. If any incident involves unauthorized disclosure or acquisition of private data, the Sheriff and IT worker must notify the Office Privacy Officer / IT Director and FA. The privacy officer will direct notification to the executive team, law enforcement and other parties as appropriate. The CD and IT workers must notify the SHE of any incident that impacts mission critical service to the enterprise. Law enforcement should be notified immediately of incidents involving threat to persons or property. The Undersheriff should be consulted regarding other incidents before contacting law enforcement. The FA, IT workers and applicable deputy chief must consult with the Office SHE and the Undersheriff to determine if law enforcement should be notified. When incidents involve law enforcement, contact the appropriate law enforcement entity and the Undersheriff. IT workers do not make disciplinary decisions unless they supervise the violator. If the incident involves an employee, notify the appropriate deputy chief and FA. In all events, follow disciplinary procedures defined by Office of the Sheriff Directives. The CD must notify the Office SHE of any incident likely to draw public interest. FIRT must be notified when any division or unit discovers an incident that poses a potential threat to other IT resources or crosses divisional boundaries to impact other divisions or units.

   d. Acknowledgment. FIRT notifications should be acknowledged immediately.
e. Containment. Suspicious activity should be contained as appropriate until the investigation is complete, or the incident is resolved. Containment can be achieved by immediately disconnecting the resource from the network, revoking user access, or other means as appropriate. Office IT workers may coordinate with the FIRT to restrict access to compromised hosts that can't be immediately disconnected or must remain connected in a restricted environment for the purpose investigation or providing service. FIRT has the authority to coordinate with Office network engineers to block compromised services and/or hosts that present a definitive danger to the rest of the network. Notification will follow the procedures outlined in the Service Interruption Notification section above.

f. Investigation: Investigation includes analysis, identification, prioritization, and evidence collection and retention.

2. Analysis: Compromised hosts must be assessed using the following process:

a. For Windows Client Computers

1) Unusual Processes and Services

i. Ensure the systems engineer running these steps are familiar with the normal processes and services on the machine and search for deviations from the norm.

ii. Look for unusual/unexpected processes by running Task Manager:
   • Start > Run and type taskmgr.exe

iii. On Windows machines, focus on processes with Username “SYSTEM” or “Administrator” (or users in the Administrator’s Group)

iv. Look for unusual started network services (GUI):
   • C:\>services.msc

2) Unusual Files and Registry Keys

i. Check file space usage to look for sudden major decreases in free space, using the GUI (right click on partition) or type:
   • C:\>dir c:\

ii. Look for unusually big files:
   • Start > Search > For Files or Folders . . . Search Options > Size > At Least 10000 KB

iii. Look for strange programs referred to in registry keys associated with system startup by running regedit:
   • HKLM\Software\Microsoft\Windows\CurrentVersion\Run
3) Unusual Network Usage

i. Look at the shares and make sure that each has a defined business purpose
   • C:\> net view \127.0.0.1
ii. Look at which sessions this machine has opened with other systems:
   • C:\> net use
iii. Look at NetBIOS over TCP/IP activity:
   • C:\>nbstat -S
iv. Look for unusual listening TCP and UDP ports
   • C:\> netstat -na
v. For continuously updated and scrolling output of this command every 5 seconds:
   • C:\> netstat -na 5
vi. For Windows Clients include the -o flag for showing owning process id:
   • C:\> netstat -nao 5
vii. Gain a general understanding of the normal port usage for the system and look for deviations.

4) Unusual Scheduled Tasks

i. On Windows, check locally scheduled tasks using the schtasks command:
   • C:\>schtasks
ii. Also check the scheduled tasks using the Task Scheduler GUI, invoked by going to Start > Programs > Accessories > System Tools > Scheduled Tasks
iii. Look for unusual scheduled items, especially those that run as a user in the Administrator’s group, as SYSTEM, or with a blank username.
iv. Look for unexpected entries in user account directories:
   • C:\Document and Settings\[username]\Start Menu\Programs\StartUp
   • C:\Winnt\Profiles\[user_name]\Start Menu\Programs\Start Up
msconfig.exe, look at Startup Tab

5) Unusual Accounts

i. Look for new, unexpected accounts in the Administrators group:
   - C:\\usrgmg.msc

ii. Click on Groups, Double Click on Administrators, then check
    members of this group

6) Unusual Log Entries

i. To look at logs, run the Windows event viewer:
   - C:\\\eventvwr.msc

ii. Or, invoke the event viewer by going to
    - Start > Program > Administrator Tools > Event Viewer

iii. Look for suspicious events, such as:

   - “Event log service was topped”
   - “Windows File Protection is not active on this system”
   - “The protected System file [file name] was not restored to its
     original, valid version because the Windows File Protection.”
   - “The MS Telnet Service has started successfully.”
   - Look for large number of failed logons attempts or locked out
     accounts.

7) Other Unusual Items

i. Look for unusually sluggish performance and a single unusual
   process hogging the CPU: Task Manager > Process and
   Performance Tabs

ii. Look for unusual system crashes, beyond the normal level for the
    given system

b. For Windows Servers

1. Unusual Processes and Services

i. Look for unusual/unexpected processes, and focus on processes
   with Username “SYSTEM” and “Administrator” (or users in the
   Administrators’ group) You need to be familiar with normal
   processes and services and search for deviations

ii. Using the GUI, run Task Manager:
- C:\> taskmgr.exe

iii. Using the command prompt:
  - C:\>tasklist
  - C:\>wmic process list full

iv. Also look for unusual services

v. Using the GUI:
  - C:\>services.msc

vi. Using the command prompt:
  - C:\> net start
  - C:\>sc query

vii. For a list of services associated with each process:
  - C:\>tasklist /svc

2. Unusual Files and Registry Keys

  i. Check file space usage to look for sudden major decreases in free space, using the GUI (right click on partition) or type:
     - C:\>dir c:\

  ii. Look for unusually big files:
     - Start > Search > For Files or Folders . . . Search Options > Size > At Least 10000 KB

  iii. Look for strange programs referred to in registry keys associated with system startup by running regedit:
     - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
     - HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
     - HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx

iv. Note that you should also check the HKCU counterparts (replace HKLM with HKCU above)

v. Using the GUI:
  - C:\> regedit

vi. Using the command prompt:
  - C:\> req query <reg key>

3. Unusual Network Usage

  i. Look at the shares and make sure that each has a defined business purpose
     - C:\> net view \127.0.0.1

  ii. Look at which sessions this machine has opened with other systems:
     - C:\> net use

  iii. Look at NetBIOS over TCP/IP activity:
     - C:\>nbstat –S
iv. Look for unusual listening TCP and UDP ports
   - C:\> netstat -na
v. For continuously updated and scrolling output of this command every 5 seconds:
   - C:\> netstat -na 5
vi. For Windows Servers include the -o flag for showing owning process id:
   - C:\> netstat -nao 5
vii. The -b flag shows the executable name and the DLLs loaded for the network connection.
   - C:\> netstat -naob 5
viii. Gain a general understanding of the normal port usage for the system and look for deviations.

4. Unusual Scheduled Tasks

   i. Look for unusual scheduled items, especially those that run as a user in the Administrator's group, as SYSTEM, or with a blank username.
   ii. Using the GUI, run Task Scheduler:
       - Start > Programs > Accessories > System Tools > Scheduled Tasks
   iii. Using the command prompt
       - C:\>schtasks
   iv. Check other AutoStart items as well, for unexpected entries, remembering to check user AutoStart directories and registry keys
   v. Using the GUI, run msconfig and look at the Start Up tab:
       - Start > Run, msconfig.exe
   vi. Using the command prompt:
       - C:\> wmic startup list full

5. Unusual Accounts

   i. Look for new, unexpected accounts in the Administrators group:
       - C:\>lusrmgr.msc
   ii. Click on Groups, Double Click on Administrators, then check members of this group
   iii. This can also be done at the command prompt:
       - C:\net user
       - C:\net local group administrators

6. Unusual Log Entries

   i. Look for suspicious events, such as:
      - "Event log service was stopped"
      - "Windows File Protection is not active on this system"
• “The protected System file [file name] was not restored to its original, valid version because the Windows File Protection.”
• “The MS Telnet Service has started successfully.”
• Look for large number of failed logons attempts or locked out accounts

ii. To look at logs, run the Windows event viewer:
  • C:\>eventvwr.msc

iii. Using the command prompt
iv. Or, invoke the event viewer by going to
  • Start > Program > Administrator Tools > Event Viewer

7. Other Unusual Items

i. Look for unusually sluggish performance and a single unusual process hogging the CPU: Task Manager > Process and Performance Tabs

ii. Look for unusual system crashes, beyond the normal level for the given system

c. Identification. Identify source as appropriate, including user, host, or other resource. FIRT must be informed of investigation details. Using the URL provided in the original notification, IT workers should access a web form for entering details about the investigation. When saved, this form will automatically notify FIRT and update the tracking system. If no URL is provided, contacts must respond to the original notification, including content of the original notification, to provide details of the investigation.

d. Evidence Collection and Retention.

1. If forensic evidence is needed for law enforcement (see Response Procedures for Incidents Involving Law Enforcement), an image of the compromised host must be retained. Email and any other relevant evidence must also be retained.

2. If the level of suspicious activities is unique or cannot be determined, evidence should be retained to aid in analysis of the incident.

g. Resolution. Suspicious activity must be resolved as soon as possible, preferably the day of the notification. Refer to the incident response procedures for Compromised IT Resources if the suspicious activity is found to be a compromise. FIRT must be informed of resolution details. Using the URL provided in the original notification, IT workers should access a web form for entering details about the resolution. When saved, this form will automatically notify FIRT and update the tracking system. If no URL is
provided, contacts must respond to the original notification, including content of the original notification, to acknowledge the resolution.

h. Postmortem Review. Prior to closing any ticket regarding an incident, FIRT must conduct a postmortem review for the purpose of the following:

1. Identify the root cause of the incident and
2. Identify the steps that need to be taken to reduce the likelihood of a repeat of this type of incident and
3. Document the operational changes that need to take place to prevent a recurrence of the incident and
4. Implement the new operational changes

i. Closure. FIRT reviews the tracking system and closes tickets as appropriate. FIRT has primary authority in response decisions for Office IT security incidents and coordinates incidents from discovery through resolution and closure. FIRT can be contacted with any questions regarding incident response.

E. Additional Incident Response Standards, Procedures, and Guidelines

1. Critical IT Resources Standard

a. A critical IT resource is vital to the function of the Office of the Sheriff. It might store sensitive data, confidential data, or data protected by law. Critical IT resources may need special consideration with respect to risk assessment, service interruption, and notification. Systems classified as critical IT resources must meet the minimum standards of a production server as defined in the “Firm Network and Host Security Standard”. Critical IT resources must be a part of the Continuity of Operations Plan (COOP) that details risk assessment, service interruption, and notification procedures. To be registered, critical IT resources must have IT personnel resources available 24 hours per day, 7 days per week.

2. Service Interruption Notification Procedures

a. The FA, Executive Team and Deputy Chiefs will be notified prior to or concurrent with a service interruption applied as the result of a security incident. Notification attempts will be made to the FA, Executive Team and Deputy Chiefs or their designees, directly by phone, beeper, or email, in that
order. Accordingly, notification may be made by way of thefirm@thefirm.com when multiple hosts are affected. An effort will be made to avoid disruption of service in cases not involving outgoing attacks.

F. Incident Tracking Standard

1. All security incidents involving Office IT resources must be tracked. The Office of the Sheriff incident tracking system is intended to monitor progress toward incident resolution and to store data that can be used for incident trend analysis. To ensure accountability and assessment, the Office IT management will provide incident trend analysis to the CD every month or as needed. The Office IT Security Team maintains an IT security incident tracking system for incidents that it processes. One ticket is created for each individual IP address or virtual domain name, or each end-user account. An IP address might have more than one ticket open at one time for different incident types, for example one host might have a vulnerability ticket and a compromise ticket. Multiple tickets might also be opened for a single IP address if more than one distinct event of the same type occurs, for example if a host is compromised by different intruder at a different time before the first incident is resolved. Ticket status may be changed at the discretion of the CD or their designee. Security incident tickets contain the following information, but are subject to change:

   a. Contacts: A list of all contacts notified about the incident. Most contacts are listed as a part of Attachment B, “The Office Contact List”.
   b. Division name.
   c. Diary: Incident details must be recorded each time the ticket is updated.
   d. Filter: Relevant information about filters associated with an incident is tracked.
   e. Incident status

   i. New: Opened, but not assigned to individual on FIRT.
   ii. Assigned: Responsibility assigned to individual on FIRT.
   iii. Contained: Threat is contained usually via some form of access restriction, but incident is not fully resolved.
   iv. Dormant: Contacts did not respond to the FIRT notification and no further activity was observed for one month. The status of tickets with associated filters cannot be changed to Dormant.
   v. Resolved: All appropriate actions have been completed.
   vi. Closed: FIRT concurs that the incident is resolved.

G. Incident severity classification (see Incident Classification Guidelines below)
1. Class 3: Any of the following.
   a. Critical Data
   b. Involves serious legal issues
   c. Service disruption impacting institution
   d. Active threat
   e. Widespread
   f. Public interest

2. Class 2: Not Class 3 and any of the following.
   a. Sensitive Data
   b. Involves less serious legal issues or potential for legal issues
   c. Service disruption impacting unit or potential for disruption impacting institution
   d. Potential for threat
   e. Somewhat widespread
   f. Potential for public interest

3. Class 1: Not Class 3 or Class 2.
   g. Unrestricted Data
   h. No legal issues
   i. No potential for service disruption impacting institution
   j. No threat
   k. Not widespread
   l. No public interest

H. Incident type

1. Vulnerability
2. Compromise/Attack
3. DMCA violation
4. AUP violation
5. Suspicious activity
6. Other

I. Operating systems of host

1. Windows
2. Macintosh
3. Unix
4. Unknown/Other
J. Incident Severity Classification Guidelines

1. Incident severity classifications are described below. Severity classifications are used for incident trend reporting. If there is any doubt about the classification of an incident, the higher severity classification should be used. Incident classifications may be changed at the discretion of the CD or their designee.

2. The following criteria are evaluated to determine incident classification.
   a. Data classification
   b. Legal issues
   c. Magnitude of service disruption
   d. Threat potential
   e. Expanse
   f. Public interest

3. To determine the severity classification for the incident tracking systems, IT workers are asked to affirm the following assertions regarding each incident.
   a. There is a reasonable expectation that critical data was acquired by an unauthorized person as a result of this incident.
   b. There is a reasonable expectation that sensitive data was acquired by an unauthorized person as a result of this incident.
   c. There is reasonable expectation that confidential or security-related information was acquired by an unauthorized person.
   d. Data protected by privacy legislation is involved.
   e. Disclosure of Office intellectual property is involved.
   f. Disclosure of ANY Office Client Information is involved.
   g. This incident involves legal violation(s).
   h. This incident impacts the Office mission critical services.
   i. There is strong potential this incident might impact Office mission critical services.
   j. There is active public interest in this incident.
   k. There is strong potential for active public interest in this incident.
   l. Hosts involved in this incident are actively attacking other hosts.
   m. There is strong potential for attack from hosts involved in this incident.
   n. This incident is widespread (over 10% of unit or greater than 100 hosts campus-wide).
   o. This incident is somewhat widespread (3-10% of unit or 10-100 hosts campus-wide).

K. Class 3: Highest Severity: If the answer is 'yes' to any of the following questions regarding an incident, then it is a Class 3 incident.
1. Data security. Is there a reasonable expectation that critical data as defined in the Office Data Security Standard was acquired by an unauthorized person as a result of this incident?

   a. Are data protected by privacy rules or legislation involved? For example:
      
      i. Social Security Number
      ii. Bank account, credit card, or other private financial information
      iii. Driver’s license number
      iv. Any medical records or protected health information as defined in HIPAA

   b. Is intellectual property involved? For example:
      
      i. Firm trade secrets

   c. Are other data security issues involved? For example:
      
      i. Passwords, risk assessments, or other security-related data.
      ii. Data restricted by legal contracts, memorandums of understanding, or other agreements.
      iii. Data, if available to unauthorized users, will cause harm to an individual, a group or the institution.

2. Legal issues. Does this incident involve any legal violation?

   a. Threat to persons or property
   b. Thefts
   c. Child pornography
   d. Copyright violations
      
      i. Warez server
      ii. Unauthorized P2P server of music, movies, or other content protected by copyright

3. Magnitude of service disruption. Does this incident impact Office mission critical services?

4. Threat. Are hosts involved in this incident actively attacking other hosts?

5. Expanse. Is this incident widespread (over 10% of unit or greater than 100 hosts campus-wide)?

6. Public interest. Is there active public interest in this incident?
L. Class 2: Medium Severity

1. If the answer is 'no' to all the Class 3 questions above, but 'yes' to any of the following questions, then it is a Class 2 incident.

   a. Data Security. Is there a reasonable expectation that Sensitive data as defined in the Office Data Security Standard was acquired by an unauthorized person as a result of this incident? For example:

      1) Infrastructure diagrams such as building and network

         i. Strategy documents
         ii. Financial information
         iii. Purchasing information
         iv. Policies, standards, and procedures
         v. Business recovery plans
         vi. System configurations
         vii. Emergency response plans
         viii. Emergency equipment inventories

   b. Legal issues. Does this incident involve a legal violation? For example:

         i. Theft
         ii. Harassment

   c. Magnitude of service disruption. Is it likely that this incident will impact The Office’s mission critical services?

   d. Threat. Is an attack likely to occur from hosts involved in this incident?

   e. Expanse. Is this incident somewhat widespread (3-10% of unit or 10-100 hosts campus-wide)?

   f. Public interest. Is there likely to be public interest in this incident?

M. Class 1: Lowest Severity

1. If an incident meets the definition in the Office IT Security Incident Response Standard above and if the answer is 'no' to all of the Class 2 and Class 3 questions above, then it is a Class 1 incident.

V. Approvals, Revisions and Receipt

A. Approvals and Revisions: These procedures and standards have been reviewed by the Sheriff. Except as otherwise stated within these written standards and procedures, the
Sheriff or Chief Deputy must approve any exceptions. The Sheriff or designee will periodically review these standards and procedures and revise this document.

B. Acknowledgment of Receipt of Policies Manual: This Information Technology Security Incident Response Procedures, Standards and Guidelines document describes important information about The Office and I understand that I should consult my manager, Senior Attorney Partner or Office Administrator of The Office regarding any questions not answered in this Procedures Manual.

C. Since the information and policies described here are necessarily subject to change, I acknowledge that revisions to this Manual may occur. All such changes will be communicated through official notices. I understand that revised information may supersede, modify, or eliminate existing procedures. Furthermore, I acknowledge that this Procedures Manual is neither a contract of employment nor a legal document.

D. Failure to follow the specific policies that are contained in this document may result in separation from The Office and/or civil action and/or criminal prosecution to the fullest extent of the law possible.

E. Approvals and Revisions: These procedures and standards have been reviewed by the Sheriff. Except as otherwise stated within these written standards and procedures, the Sheriff or Chief Deputy must approve any exceptions. The Sheriff or designee will periodically review these standards and procedures and revise this document.

F. Approvals and Revisions: These procedures and standards have been reviewed by the Sheriff. Except as otherwise stated within these written standards and procedures, the Sheriff or Chief Deputy must approve any exceptions. The Sheriff or designee will periodically review these standards and procedures and revise this document.

G. Acknowledgment of Receipt of Policies Manual:

This Information Technology Security Incident Response Procedures, Standards and Guidelines document describes important information about The Office, and I understand that I should consult my manager, Senior Attorney Partner or Office Administrator of The Office regarding any questions not answered in this Procedures Manual.
Since the information and policies described here are necessarily subject to change, I acknowledge that revisions to this Manual may occur. All such changes will be communicated through official notices. I understand that revised information may supersede, modify, or eliminate existing procedures. Furthermore, I acknowledge that this Procedures Manual is neither a contract of employment nor a legal document.

Failure to follow the specific policies that are contained in this document may result in separation from The Office and/or civil action and/or criminal prosecution to the fullest extent of the law possible.

I have received the Procedures Manual and I understand that it is my responsibility to read and comply with the policies contained in it and any revisions made to it.

Consultant/Employee’s Signature: ___________________________ Date: ________________

Consultant/Employee’s Manager Signature: ___________________________ Date: ________________
Appendix A

I. Office Network and Host Security Standard and Procedures

A. Access to Office IT resources must be restricted to authorized methods. Facilities must be established to identify who was using any node on the network and when they were doing so. Access methods must be sanctioned by the FA. Access must be logged, and each log entry must include user identification, network address, hardware address, and an accurate time stamp. Logs must be regularly reviewed for anomalies including unauthorized access. Access logs must be retained for at least six months unless required by law to be retained longer.

B. The CD or his designee must establish and document criteria for issuing and revoking accounts used for access.

II. Network Security Standard

A. Nodes, services, and individuals shall not have network exposure and visibility beyond that which is necessary for their intended functions. Similar IT resources should be logically aggregated to facilitate network security zone management. In cases where network firewalls are used, they must be documented and coordinated with Office network engineers.

B. As every external network connection is potentially an entry point for intruders, the Office IT will coordinate and document the establishment of all external network connections.

C. Only network access locations designated by the Office CD may be used by personally managed IT resources. Office IT are responsible for all network access locations used by personally managed IT resources but are not responsible for the resources themselves. Office IT has the responsibility to identify a user connected to a given port at any given time. Office IT must be able to instigate disruption of service to the user and/or address. Office IT also has the responsibility to coordinate notification to the user and ensure that the incident is resolved.

D. Network access for personally managed IT resources should be more restricted than network access for professionally managed IT resources. Possible restrictions include:

1. WIPA authentication where possible.
2. A VLAN separate from the professionally managed machines.
3. Restriction to private IP only.
4. Incoming and outgoing network firewalls or access control lists to prevent commonly exploited network services.
5. Restrictions that prevent external hosts from initiating connections.

III. Node Security Standard

A. Before connecting to the Office network, devices managed by Office IT workers must:

1. Have a clearly defined Office purpose and intended user base.
2. Be protected during the installation process by some combination of restricted network access, specific ACLs, private IP, or off-line installation (Best Practices for Secure Installation).
3. Be operated and secured appropriately for its specified network zone.
4. Have appropriate access restrictions, including but not limited to physical, ACL, firewall, authentication, authorization restrictions, screen locks, and inactivity timeouts. Network restrictions must allow access to the Office security scanner.
5. Be on private IP unless public IP is required. *
6. Be at current patch levels. *
7. Have current anti-malware protection. *
8. Have current and operable personal firewall *
9. Have a specific individual designated as manager.
10. Be documented for recreating the system. *
11. Be documented for operating the system and troubleshooting. *
12. Have alerting and/or logging for security-related events or patterns where appropriate.
13. Be reviewed for security-related events or patterns with a frequency appropriate to the system.
14. Run only the services necessary to support its function.
15. Run only software necessary to support its function. *
16. Be monitored for proper system operation where appropriate. *
17. Provide system facilities to allow users to secure their data. *
18. Have been scanned for vulnerabilities within the last 3 months.
19. Comply with appropriate Software Security Standard(s).
20. Comply with appropriate Data Security Standard(s).
21. Have defined power and backup power requirements where appropriate. *
22. Have defined heat generation data where appropriate. *
23. Not have trust relationships beyond those required for proper function. Where needed, trust relationships should be based on secure cryptographic methods (e.g., SSH public keys or SSL certificates), and not on IP numbers or domain names alone. *
24. Be synchronized with an accurate time server. *

B. This standard recognizes that there is more than one way to secure a device. Alternative methods to secure a device may be used where it is not possible to implement this standard or it interferes with proper device function. In addition, production servers must:

1. Be in The Office’s data center space.
2. Be routinely backed up, use off-site backup storage, and document restoration testing as appropriate.
IV. Software Security Standard

A. It is the responsibility of the RITM to ensure that all software used by The Office is properly licensed. Department heads must ensure that users in their departments are properly informed of their responsibilities regarding legal use of software. The CD has the responsibility to request the removal of software that does not comply with licensing agreements or copyright law, but it is the responsibility of the user to comply with licensing agreements and copyright law as defined in the Office Acceptable Use Policy.

B. Office IT workers must be aware of and comply with applicable laws and policies regarding their use of software on IT resources they manage. All software systems must be as robust against unauthorized use or attack as is possible consistent with providing necessary services.

C. A means for scanning every IT resource for invasive or malicious software must be provided. The CD or his designee has the authority and responsibility to ensure an appropriate level of security of computer applications developed at or intended for use at The Office for processing financial data, client data, employee data, health data, mission critical data, intellectual property or any other data that is Sensitive and Critical. This applies to the development process as well as to the deployment process. It is particularly critical for network applications. Unless the CD has instituted alternative guidelines, it is incumbent upon the developer to demonstrate to the CD or his designee that they follow secure application development procedures. Security must be considered throughout the coding life cycle including design, implementation, testing, auditing, and improvement.

D. A secure application:

1. Is auditable, both in source code and in actual use.
2. Has its design and implementation reviewed by experienced practitioners.
3. Does not rely on just one layer of security.
4. Has been tested against malicious usage and in general, follows Office Procedures to Develop Applications for Secure Deployment.

V. Change Management Security Standard

A. Changes to IT resources must be planned, documented, and announced to the appropriate audience. The planning must consider the impact on confidentiality, integrity, availability, recoverability, and auditability.

VI. Data Security Standard

A. All Office Data must be classified according to the Office Data Classification Schema and protected according to the Office Data Security Standards.

1. Responsibility for Data Management
a. Data is a critical asset of The Office (The Firm). All members of The Office community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by The Firm, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form).

b. Departments are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of The Office data in compliance with this policy.

c. Data owned, used, created, or maintained by The Office is classified into the following three categories:

1. Public
2. Restricted
3. Private
4. Sensitive
5. Confidential

d. Divisions should carefully evaluate the appropriate data classification category for their information.

e. When provided in this policy, examples are illustrative only, and serve as identification of implementation practices rather than specific requirements. Nothing in this policy is intended to identify a restriction on the right of departments to require policies and/or procedures in addition to the ones identified in this document.

2. Data Classifications

a. Public Data

1) Public data is information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data, while subject to The Office disclosure rules, is available to all members of The Office community and to all individuals and entities external to The Office community.

2) By way of illustration only, some examples of Public Data include:

   i. Publicly posted press releases
   ii. Publicly posted fee / rate schedules
   iii. Publicly posted interactive The Office maps, newsletters, newspapers, and magazines
   iv. Public areas of The Office websites

b. Restricted Data
1) Restricted Data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage, or other use. This classification applies even though there may not be a civil statute requiring this protection. Restricted Data is information that is restricted to members of The Office community who have a legitimate purpose for accessing such data.

2) By way of illustration only, some examples of Restricted Data include:

   i. The Office partner or sponsor information where no more restrictive confidentiality agreement exists
   ii. Internal telephone books and directories
   iii. Internal Processes and Procedures
   iv. Internal Policy documentation
   v. Internal E-Mail and other Internal documentation and memorandum

3) Restricted Data:

   i. Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
   ii. Must not be posted on any public website.
   iii. Must be destroyed when no longer needed subject to The Office’s Records Management Policy. Destruction may be accomplished by:

      - "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
      - Electronic storage media shall be sanitized appropriately by overwriting or degaussing prior to disposal.

   c. Private Data

1) Private Data is information protected by statutes, regulations, The Office policies, or contractual language. Managers may also designate data as Private. Private Data may be disclosed to individuals on a need-to-know basis only. Disclosure to parties outside The Office should be authorized by executive management.

2) By way of illustration only, some examples of Private Data include:

   i. The Office COOP or Business Plans
   ii. Employment Data
   iii. The Purchasing Office Client Contracts and Agreements

3) Private data:
i. Must be stored in a closed locking container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.

ii. When stored in an electronic format, must be protected with strong passwords, and stored on servers that have protection and encryption measures provided by DivIT in order to protect against loss, theft, unauthorized access, and unauthorized disclosure.

iii. Must not be disclosed to parties without explicit management authorization.

iv. Must be stored only in a locked drawer or room or an area where access is controlled by sufficient physical access control measures to afford adequate protection and prevent unauthorized access by employees or members of the public, visitors, or other persons without a need-to-know.

v. When sent via fax must be sent only to a previously established and used address or one that has been verified as using a secured location.

vi. Must not be posted on any public website.

vii. Must be destroyed when no longer needed subject to The Office’s Records Management Policy. Destruction may be accomplished by:

- "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
- Electronic storage media shall be sanitized appropriately by overwriting or degaussing prior to disposal.

d. Sensitive Data

1) Sensitive Data is information protected by statutes, regulations, The Office’s policies, or contractual language. Managers may also designate data as Sensitive. Sensitive Data may be disclosed to individuals on a need-to-know basis only. Disclosure to parties outside The Office should be authorized by Executive Management only.

2) By way of illustration only, some examples of Sensitive Data include:

   i. Employee Contact Information
   ii. Background Check Information
   iii. The Office Legal Information
   iv. The Office Client Contact Information

3) Sensitive data:

   i. When stored in an electronic format, must be protected with strong passwords, and stored on servers that have protection and encryption measures provided by The Office IT in order to protect against loss, theft, unauthorized access, and unauthorized disclosure.
ii. Must not be disclosed to parties without explicit management authorization.

iii. Must be stored only in a locked drawer or room or an area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.

iv. When sent via fax must be sent only to a previously established and used address or one that has been verified as using a secured location.

v. When sent via e-mail must be sent only via encrypted e-mail to a previously established and used e-mail address or one that has been verified as using a secured location.

vi. Must not be posted on any public website.

vii. Must be destroyed when no longer needed subject to The Office’s Records Management Policy. Destruction may be accomplished by:

   - "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
   - Electronic storage media shall be sanitized appropriately by degaussing prior to disposal. Hard drives and other magnetic media containing confidential data must be certified as shredded with an auditable chain of custody of the media.

e. Confidential Data

1) Confidential Data is information protected by statutes, regulations, The Office policies, or contractual language. Managers may also designate data as Confidential. Confidential Data is also any and all The Office client data regardless of how The Office’s clients classify that data. Confidential Data may be disclosed to individuals on a need-to-know basis only. Disclosure to parties outside The Office should be specifically authorized by the Executive Management Team and/or the Undersheriff.

2) By way of illustration only, some examples of Confidential Data include:

   i. Medical records
   ii. Client records and other non-public client data
   iii. Social Security Numbers
   iv. Personnel and/or payroll or records
   v. Bank account numbers and other personal financial information
   vi. Driver’s License numbers
   vii. Any data identified by government regulation to be treated as confidential or sealed by order of a court of competent jurisdiction.
3) Confidential data:

   i. When stored in an electronic format, must be protected with strong passwords, and stored on servers that have protection and encryption measures provided by The Office IT in order to protect against loss, theft, unauthorized access, and unauthorized disclosure.
   
   ii. Must not be disclosed to parties without explicit management authorization.
   
   iii. Must be stored only in a locked drawer or room or an area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.

- When sent via fax must be sent only to a previously established and used address or one that has been verified as using a secured location.
- When sent via e-mail must be sent only via encrypted e-mail to a previously established and used e-mail address or one that has been verified as using a secured location.
- Must not be posted on any public website.
- Must be destroyed when no longer needed subject to The Office’s Records Management Policy. Destruction may be accomplished by:

  o "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
  
  o Electronic storage media shall be sanitized appropriately by degaussing prior to disposal. Hard drives and other magnetic media containing confidential data must be certified as shredded with an auditable chain of custody of the media.

4) The Office CD must be notified in a timely manner if data classified as Private, Sensitive and/or Confidential is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of The Office’s information systems has taken place or is suspected of taking place.

5) To prevent confidential data loss, the use of portable media to move / copy data is strictly prohibited, and security policies are in place to disable the use of portable media devices on all The Office’s workstations

3. Data Classification Roles and Responsibilities

a. The Chief Deputy is the Chief Operating Officer, and is the primary entity charged with developing policy and procedures subordinate to and in support of this policy.
b. The IT Director and Chief Operating Officer is charged with the promotion of security awareness within The Office community, as well as responsibility for the creation, maintenance, enforcement, and design of training on relevant security standards in support of this policy.

c. The IT Director will receive and maintain reports of incidents, threats and malfunction that may have a security impact on The Office’s information systems and will recommend and maintain records of actions taken or policies and procedures developed in response to such reports.

d. The Internal Affairs Deputy Chief will assist in conducting periodic audits to determine The Office compliance with this policy.

4. Data Security Standards

a. The following table defines requisite safeguards for protecting data based on its classification.

An audit of compliance with the requirements in the following table must be performed according to the schedule listed in the table:

<table>
<thead>
<tr>
<th>Access Controls</th>
<th>Public</th>
<th>Restricted/Private Data</th>
<th>Sensitive Data</th>
<th>Confidential Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No restriction for viewing.</td>
<td>Viewing and modification restricted to authorized individuals</td>
<td>Viewing and modification restricted to authorized individuals</td>
<td>Viewing and modification restricted to authorized individuals</td>
</tr>
<tr>
<td></td>
<td>Authentication required for modification</td>
<td>Data Steward grants permission for access, plus approval from supervisor</td>
<td>Data Steward grants permission for access, plus approval from supervisor</td>
<td>Data Steward grants permission for access, plus approval from supervisor</td>
</tr>
<tr>
<td></td>
<td>Data Steward grants permission for modification, plus approval from supervisor</td>
<td>Authentication required for access</td>
<td>Authentication required for access</td>
<td>Authentication required for access</td>
</tr>
<tr>
<td>Copying/Printing</td>
<td>No restrictions</td>
<td>Data should only be printed</td>
<td>Data should only be printed</td>
<td>Data should only be printed</td>
</tr>
</tbody>
</table>

365
<table>
<thead>
<tr>
<th>Public</th>
<th>Restricted/Private Data</th>
<th>Sensitive Data</th>
<th>Confidential Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>when there is a legitimate need</td>
<td>when there is a legitimate need</td>
<td>when there is a legitimate need</td>
<td>when there is a legitimate need</td>
</tr>
<tr>
<td>Copies must be limited to individuals with a need to know</td>
<td>Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement</td>
<td>Copies must be stamped with “Confidential” or have a cover sheet indicating “Confidential”</td>
<td>Copies must be stamped with “Confidential” or have a cover sheet indicating “Confidential”</td>
</tr>
<tr>
<td>Data should not be sent to an unattended printer or left sitting on a printer</td>
<td>Data should not be sent to an unattended printer or left sitting on a printer</td>
<td>Data should not be sent to an unattended printer or left sitting on a printer</td>
<td>Data should not be sent to an unattended printer or left sitting on a printer</td>
</tr>
<tr>
<td>Protection with a firewall required</td>
<td>Protection with a firewall using “default deny” ruleset required</td>
<td>Protection with a firewall using “default deny” ruleset required</td>
<td>Protection with a firewall using “default deny” ruleset required</td>
</tr>
<tr>
<td>Protection with a firewall required</td>
<td>Protection with a firewall using “default deny” ruleset required</td>
<td>Protection with a firewall using “default deny” ruleset required</td>
<td>Protection with a firewall using “default deny” ruleset required</td>
</tr>
<tr>
<td>Protection with a firewall required</td>
<td>Protection with a firewall using “default deny” ruleset required</td>
<td>Protection with a firewall using “default deny” ruleset required</td>
<td>Protection with a firewall using “default deny” ruleset required</td>
</tr>
<tr>
<td>IDS/IPS protection required</td>
<td>IDS/IPS protection required</td>
<td>IDS/IPS protection required</td>
<td>IDS/IPS protection required</td>
</tr>
<tr>
<td>IDS/IPS protection required</td>
<td>IDS/IPS protection required</td>
<td>IDS/IPS protection required</td>
<td>IDS/IPS protection required</td>
</tr>
<tr>
<td>Protection only with router ACLs not acceptable</td>
<td>Protection only with router ACLs not acceptable</td>
<td>Protection only with router ACLs not acceptable</td>
<td>Protection only with router ACLs not acceptable</td>
</tr>
<tr>
<td>Protection only with router ACLs not acceptable</td>
<td>Protection only with router ACLs not acceptable</td>
<td>Protection only with router ACLs not acceptable</td>
<td>Protection only with router ACLs not acceptable</td>
</tr>
<tr>
<td>Service should not be visible to entire Internet, but can be if necessary</td>
<td>Servers storing the data cannot be visible to the entire Internet</td>
<td>Servers storing the data cannot be visible to the entire Internet</td>
<td>Servers storing the data cannot be visible to the entire Internet</td>
</tr>
<tr>
<td>Servers storing the data cannot be visible to the entire Internet</td>
<td>Servers storing the data cannot be visible to the entire Internet</td>
<td>Servers storing the data cannot be visible to the entire Internet</td>
<td>Servers storing the data cannot be visible to the entire Internet</td>
</tr>
<tr>
<td></td>
<td>Public</td>
<td>Restricted / Private Data</td>
<td>Sensitive Data</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>System Security</strong></td>
<td>Follows general best practices for system management and security</td>
<td>Must follow Firm-specific and OS-specific best practices for system management and security</td>
<td>Must follow Firm-specific and OS-specific best practices for system management and security</td>
</tr>
<tr>
<td></td>
<td>Host-based software firewall recommended</td>
<td>Host-based software firewall required</td>
<td>Host-based software firewall required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Host-based software IDS/IPS recommended</td>
<td>Host-based software IDS/IPS required</td>
</tr>
<tr>
<td><strong>Physical Security</strong></td>
<td>System must be locked or logged out when unattended</td>
<td>System must be in a secure location</td>
<td>Access monitored and limited to authorized individuals 24x7</td>
</tr>
<tr>
<td></td>
<td>Secure Data Center recommended</td>
<td>System must be locked or logged out when unattended</td>
<td>All physical access must be logged</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure Data Center recommended</td>
<td>System must be locked or logged out when unattended</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Secure Data Center required</td>
</tr>
</tbody>
</table>

367
<table>
<thead>
<tr>
<th></th>
<th>Public</th>
<th>Restricted/ Private Data</th>
<th>Sensitive Data</th>
<th>Confidential Data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remote Access</strong></td>
<td>No restrictions</td>
<td>Restricted to local network or general Office Virtual Private Network (VPN) service</td>
<td>Restricted to local network or secure VPN group</td>
<td>Restricted to local network or secure VPN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote access by third party for technical support limited to authenticated, temporary access via dial-in modem or secure protocols over the Internet</td>
<td>Two-factor authentication recommended</td>
<td>Two-factor authentication required</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Remote access by third party for technical support not allowed</td>
<td>Remote access by third party for technical support not allowed</td>
</tr>
<tr>
<td><strong>Storage</strong></td>
<td>No requirements</td>
<td>Storage on a secure server recommended</td>
<td>Storage on a secure server in a secure Data Center required.</td>
<td>Storage on a secure server in a secure Data Center required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Storage in a secure Data Center recommended</td>
<td>Must not store on an individual’s workstation</td>
<td>Must not store on an individual workstation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Should not store data on an individual’s workstation</td>
<td>Must be encrypted if stored on a mobile device</td>
<td>Must not store on a mobile device (e.g. a laptop computer)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Encryption recommended</td>
<td>Encryption required</td>
</tr>
<tr>
<td><strong>Transmission</strong></td>
<td>No requirements</td>
<td>No requirements</td>
<td>Secure protocols required</td>
<td>Secure protocols required</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cannot transmit via e-mail</td>
<td>Cannot transmit via e-mail</td>
</tr>
<tr>
<td><strong>Backup/Disaster Recovery</strong></td>
<td>Data should be backed up daily</td>
<td>Daily backups required</td>
<td>Daily backups required</td>
<td>Daily backups required</td>
</tr>
<tr>
<td></td>
<td>Public</td>
<td>Restricted / Private Data</td>
<td>Sensitive Data</td>
<td>Confidential Data</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------</td>
<td>----------------------------</td>
<td>----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Data Disposal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>If system will be re-used: Format hard drive(s)</td>
<td></td>
<td>If system will be re-used: Overwrite data at least once so is not recoverable</td>
<td>Off-site storage in a secure location required</td>
<td>Off-site storage in a secure location required</td>
</tr>
<tr>
<td>If system will not be re-used: no requirements</td>
<td></td>
<td>If system will not be re-used: Overwrite or destroy (e.g. degauss) data so is not recoverable, or physically destroy the media</td>
<td>Encrypted backups recommended</td>
<td>Encrypted backups required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If system will not be re-used: Overwrite or destroy (e.g. degauss) data so is not recoverable, or physically destroy the media</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td>General security awareness training recommended</td>
<td>General security awareness training required</td>
<td>General security awareness training required</td>
<td>General security awareness training required</td>
</tr>
<tr>
<td></td>
<td>System administration training recommended</td>
<td>System administration training required</td>
<td>System administration training required</td>
<td>System administration training required</td>
</tr>
<tr>
<td></td>
<td>Data security training recommended</td>
<td>Data security training required</td>
<td>Data security training required</td>
<td>Data security training required</td>
</tr>
<tr>
<td>Audit Schedule</td>
<td>As needed</td>
<td>As needed</td>
<td>Annual</td>
<td>Semi-annual</td>
</tr>
</tbody>
</table>
Appendix B

I. Summary of Response Procedures for Incidents Involving Law Enforcement entities.

A. Examples: obscenity, stalking, threat to persons or property, child pornography, unauthorized access.

1. Evidence retention. Secure evidence without reviewing additional content. Network hardware, software or data may be considered evidence. Care must be taken to preserve evidence.

2. Evidence release. A public records request, subpoena, warrant or other official request must be issued before data is released to law enforcement. Contact the Undersheriff to review public records requests, subpoenas, and warrants before responding. Evidence from incidents that involve an immediate threat to persons or property may be provided to law enforcement in advance of a public records request, subpoena, or warrant, but the Undersheriff shall be contacted.

3. Notifications. If any incident involves unauthorized disclosure or acquisition of private data, IT workers must notify the CD and the CD must notify the Office Privacy Officer / IT Director. The privacy officer will direct notification to the executive team, law enforcement and other parties as appropriate. IT workers must notify the CD and the CD must notify the SHE of any incident that impacts mission critical service to the enterprise level. The appropriate law enforcement entity will be notified of incidents involving an immediate threat to persons or property. The Undersheriff should be consulted regarding other incidents before contacting law enforcement. The CD must consult with the Undersheriff to determine if law enforcement should be notified. When incidents involve a law enforcement entity, contact the appropriate police department or law enforcement entity and the Undersheriff. If the incident involves an employee, notify the appropriate Deputy Chief. IT workers do not make disciplinary decisions unless they supervise the violator. In all events, follow Office disciplinary procedures defined by Office of the Sheriff directives. The CD must notify the SHE of any incident likely to draw public interest.
Appendix C

I. Summary of Incident Response for Legal Issues

A. Examples: defamation, civil fraud, harassment, disclosure of intellectual property or illegal or unauthorized transmissions of office trade secrets.

1. Evidence retention. Secure evidence without reviewing additional content and contact the Undersheriff.

2. Notifications. If any incident involves unauthorized disclosure or acquisition of private data, IT workers and the CD must notify the Office Privacy Officer / IT Director. The privacy officer will direct notification to other members of the Office executive team, law enforcement and other parties as appropriate. The CD must notify the SHE of any incident that impacts mission critical service to the enterprise level. IT workers do not make disciplinary decisions unless they supervise the violator. If the incident involves an employee, notify the appropriate Director or Department Head. In all events, follow Office disciplinary procedures defined by Office Human Resources. IT workers and the CD must notify the Office SHE of any incident likely to draw public interest.
Appendix D

I. Summary of Internal and Public Communication Notification Procedures

A. Upon receipt of notifications from FIRT, employees, executive, suppliers, and stakeholders must respond as directed in the notification. All divisions must notify FIRT immediately upon discovery of security incidents in their division that impact resources outside their divisions.

B. If any incident involves unauthorized disclosure or acquisition of private data, FA, IT workers and Deputy Chiefs must notify the Office Privacy Officer / IT Director. The privacy officer will direct notification to the executive team, clients and law enforcement and other parties as appropriate. The CD must notify the SHE of any incident that impacts mission critical service to the enterprise level.

C. When evidence of a possible crime is discovered, IT workers should report it to their supervisors. Supervisors should escalate communication through normal channels in their division but must contact the CD and their respective Deputy Chief.

D. Deputy Chiefs must be notified regarding any incident within their division. The CD should consult with the Undersheriff before reporting an incident to the appropriate law enforcement entity unless there is an immediate threat to persons or property.

E. The CD shall consult the Undersheriff before responding to public records requests, subpoenas, warrants or other requests for assistance from law enforcement entities unless there is an immediate threat to persons or property. The CD should consult either the SHE or Undersheriff if there is any doubt about whether an incident should be reported to law enforcement.

F. Law enforcement shall be notified of incidents involving:

1. Threats to persons or property.

2. Any damage to Office of the Sheriff property.

3. Child pornography.

4. Other incidents should be reported to law enforcement according to the judgment of the FA. The SHE must be consulted and notified before responding to any inquiry from the press. IT workers and the SHE must consult the Sheriff, IT Director, Office SHE and designated Communications Officer regarding any incident that draws public attention or is expected to draw public attention.
Attachment A.A - Key FIRT Contact Information

The members of the FIRT are as follows:

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Company</th>
<th>Title</th>
<th>Office Phone</th>
<th>Cell Phone</th>
<th>Home Phone</th>
<th>E-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td></td>
<td>Sheriff</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td></td>
<td>Chief Deputy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
<td>vCTO/vCI SO/ IT Director</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td></td>
<td>Undersheriff/Firm Privacy Officer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td></td>
<td>Communications Officer or designee</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Attachment A.B – The Office Contact List

Notes:

BY ORDER OF:

[Signature]
SHERIFF  DATE
Philadelphia Sheriff's Office

DIRECTIVE: #49
SUBJECT: CIVILIAN GRIEVANCES
ISSUE DATE: 03-17-2020
REvised DATE: 02-18-2021

LX. POLICY:

A. It is the policy of the Philadelphia Office of the Sheriff to settle grievances fairly and in good faith. It is also the policy of this Office to attempt to settle such grievances in an amicable, informal setting whenever possible.

LXI. PROCEDURE:

A. Due to the contractual relationships established with AFSCME District Councils 33 and 47, the following procedural instructions will serve as a guide in the grievance procedure for both unions.

B. All unit heads and managers will refer to/adhere to the contractual guidelines when handling matters of this nature.

BY ORDER OF:

[Signature]
SHERIFF
DATE
LXII. POLICY:

B. It is the policy of the Philadelphia Sheriff’s Office to release information that is public pursuant to existing Commonwealth of Pennsylvania Freedom of Information ACT (FOIA) request law.

1. Media: Refers to all Reporters, Photographers, Camera Operators and Others who are directly employed by agencies of the media and who hold valid news media identification/credentials.

   a. Entities related to media outlets, such as Crime Stoppers, are considered related outlets for purposes of this policy.

2. Except as may otherwise be authorized by the Sheriff or his/her designee, employees shall not release information to the media or related outlets other than as prescribed by this directive.

   a. Exception: The release of information responsive to a Freedom of Information Act request or records subpoena shall be coordinated through the Undersheriff.

3. The Public Information Deputy and Chief of Staff work to promote effective relations between the media and the Office of the Sheriff.

C. The Public Information Deputy and/or Chief of Staff shall promote effective relations between the news media and the Philadelphia Office of the Sheriff by:

1. Assisting the media in covering news stories at the scene of Sheriff’s operations.

2. Preparing and distributing news releases.
3. Arranging for, and assisting at, news conferences.

4. Coordinating and authorizing the release of information.

5. Coordinating the release of information with other public service agencies.

LXIII. **PROCEDURE:**

A. The general function of the Public Information Deputy shall include but not necessarily be limited to:

1. Assisting news personnel in covering news stories at the scenes of incidents.

2. Distributing public safety information via social media channels.

3. Being available for on-call responses to the news media.

4. Preparing and distributing agency news releases.

5. Arranging for and assisting at news conferences.

6. Coordinating and authorizing the release of information about victims, witnesses, and suspects.

7. Assisting in crisis situations within the agency.

8. Coordinating and authorizing the release of information concerning agency investigations and operations.

9. Developing procedures for releasing information when other public service agencies are involved in a mutual effort.

B. The Public Information Officer (PIO) works under the Undersheriff and is authorized to act as the representatives of the Sheriff to members of the media.

C. Non-authorized personnel shall not provide any information to the media.

D. When the media requests an interview with an on-duty employee, the deputy shall refer media representatives to the PIO, their respective captain, lieutenant, or Deputy Chief.

E. Deputy Involved Critical Incidents:

1. At incidents where the media is on-scene and a PIO is not available, the facility Captain or Deputy Chief of Uniform Operations may be authorized by the Sheriff or Chief Deputy to speak to the media on behalf of the Office of the Sheriff.
2. When the media does not respond to the scene but then contacts an Office employee when there is not a PIO on-duty, the employee shall instruct the media to call the on call IAD Supervisor, who will contact the on-call PIO.

3. The on-call PIO will communicate directly with news outlets regarding non-urgent matters as needed.

F. The Sheriff is the only person authorized to speak to the media regarding Office of the Sheriff’s budget issues, Office Goals, Allocation of Resources, and the Interpretation of Office Directives or Policies.

G. Deputies will notify the PIO of all requests for interviews and get approval, prior to speaking with the media.

1. If a time constraint exists, the on call IAD Supervisor will call (or contact via Everbridge) the on-call PIO to screen the incident.

2. It is the responsibility of the deputy, and deputy’s supervisor that deputy to notify the next level up supervisor when at or responding to an incident that is likely to result in a media response or when notification of the PIO is required by directive.

3. If the incident is an in-progress Deputy Chief of Operations, the on-scene captain or permanent-rank lieutenant will contact highest ranking supervisor working (or the on call IAD Supervisor) and request that a PIO respond to the scene.

   a. At the Sheriff’s discretion, the highest-ranking supervisor working may act as the Philadelphia Sheriff’s Office media representative if a PIO does not respond.
   b. The highest-ranking supervisor working will send a notification to the PIO via email account to document the tenets of the interview.

H. Interaction with the Media

1. Authorized Philadelphia Office of the Sheriff employees shall cooperate with representatives of the media in a courteous and professional manner, providing only accurate, objective, factual responses that are consistent with this directive.

2. Authorized employees shall speak about the facts as you know them. Do not speculate or editorialize. If you do not know the answer to a question, refer the media person to someone who has that information or tell them that you will attempt to get the information and get back to them.

   a. Take time in answering questions and give a thoughtful response.
   b. Do not make off-the-record statements to the media. The media is under no obligation to keep your statement off the record.
c. Philadelphia Office of the Sheriff's employees should contact the PIO with any complaint they have about an interaction with the media.

LXIV. MISCELLANEOUS:

A. Prisoners: Philadelphia Office of the Sheriff's employees shall neither prevent nor facilitate the photographing of defendants or suspects in custody.

B. Ride-A-Longs/Shadows: The Chief Deputy shall coordinate requests for media ride-a-long, or deputy sheriff shadowing.

1. The Public Information Officer shall ensure that the facility hosting the media representative complete and sign a Civilian Observer Ride Request and Waiver.

2. During the ride-along, the media representative will not be allowed to use any image-recording device or audio recorder without the prior approval of the Sheriff.

C. Release of Information to the Media

1. The Sheriff, Chief Deputy and the Undersheriff will screen the information that will be released to the media in a Deputy Involved Shooting or Deputy Involved Critical Incident (DICl) where a serious injury or death of a person occurs as a result of law enforcement activity.

2. The Philadelphia Office of the Sheriff will generally release information to the media in a timely manner.

3. The Public Affairs Unit will be the conduit for releasing information to the media. Public Affairs will coordinate with follow-up units when applicable to verify the case status and ensure that information released will not compromise an on-going investigation or pending prosecution. Information that is publicly available will be released as needed.

4. For additional information regarding the release of information related to any deputy-involved shooting, see Directive 1: Use of Force.

5. All media outlets have equal access to Philadelphia Sheriff's Office information once it has been deemed acceptable for release.

6. There is certain information that can generally be released to the media:

   a. The facts regarding an incident that may include:

      1) A basic description of the incident
      2) How the incident came to Philadelphia Sheriff's Office attention.
3) What time the Philadelphia Sheriff's Office responded to the call.
4) How many deputies are currently assigned to the call?
5) The number of suspects and victims involved in the incident.

b. Adult suspects charged with a crime:

1) Suspect's name, age, gender, race, and city of residence
2) Charge filed by Philadelphia Sheriff's Office and approved/denied by the Philadelphia Office of the District Attorney
3) Arresting/investigating unit
4) Circumstances of the arrest
5) Adult suspects who have been arrested and booked into jail or cited but not charged with a crime:

c. Suspect's name, age, gender, race, and city of residence

1) Alleged offense
2) Arresting/investigating unit
3) Circumstances of the arrest

d. Adult suspects who have been arrested, not booked into jail, or cited, and have not been charged with a crime:

1) Age, gender, race, and city of residence
2) Investigating/arresting agency

e. Medical condition of a suspect/victim:

1) Readily observed information regarding medical conditions may be released.
2) Detailed medical information, diagnosis or prognosis will not be released.

f. Deceased persons:

1) Only the age, gender, race, and city of residence of the deceased person may be released.
2) The Philadelphia County Medical Examiner's Office and/or the PPD Homicide Unit will be responsible for releasing the identification of the deceased person.

g. Information Pertaining to Juveniles, their Parents, or Legal Guardians Will Not Be Released

1) This applies whether the juvenile is reported as a suspect, witness, victim, missing person, runaway or person of interest.
2) Information identifying child victims under age eighteen who are victims of sexual assault is confidential and not subject to release to the press or public.

3) Photographs of juveniles will not be released to the media without a court order or the consent of the juvenile’s parent or guardian.

7. Certain information will generally not be released to the media unless authorized by the Sheriff, Chief Deputy or Undersheriff:

   a. Statements about a suspect or defendant’s:

      1) Character, criminal record, or reputation in the community
      2) Guilt, innocence, or possible outcome of pending legal proceedings

   b. The existence or content of any admission, confession, or alibi.

   c. Statements or opinions regarding a defendant’s willingness or refusal to make a statement.

   d. The results of evidentiary examinations or forensic tests involving a pending case.

   e. The anticipated testimony or credibility of any prospective victim or witness.

   f. Statements or opinions concerning evidence, or legal arguments, to be used in a pending case.

   g. Information regarding bombings, bomb threats, kidnappings, or kidnapping threats, unless authorized by the Sheriff, Chief Deputy, or Undersheriff.

   h. Any information disclosing the identity of a confidential source

   i. Identification information related to the victim of a sexual assault

8. Information on Vehicular Accidents:

   a. will be restricted to the narrative portion of the Incident Report and must be requested thorough the Chief of Staff.

   b. The names, license numbers or registration numbers of the persons and vehicles involved in the collision will not be released.

9. Booking photo(s) or an investigative file photo(s) of a suspect(s) wanted for a serious crime may be released to the media if it will assist in the capture of the suspect or warn the public if the suspect is a danger to the community or themselves.
a. Authorization to release the photograph must come from the PPD unit investigating the crime.

10. Photographs of Sex Offenders may be released to the media and the public.

11. The home address, telephone number, or date of birth of any department employee will not be released without the employee’s expressed consent.

12. The release of immediate on-scene information of the involved employee will be confined to the employee’s age, race, gender, rank, tenure, and division/facility of assignment.

13. Media Representatives may obtain copies of incident reports through the PIO or the Chief of Staff.

BY ORDER OF:

[Signature]

SHERIFF DATE
DIRECTIVE:  #51
SUBJECT:  RESPONDING TO REQUESTS FROM ELECTED OFFICIALS
ISSUE DATE:  04-16-2020
REVISED DATE:  04-16-2020

LXV. PURPOSE:

J. This policy applies to all forms of communication by all civilian employees below the rank of executive and all sworn employees below the rank Chief Deputy, Undersheriff, and Chief of Staff. Personnel conducting community meetings may communicate with elected officials, as appropriate.

K. The Sheriff’s Office shall ensure a prompt and thorough response to contacts and requests from elected officials and their representatives.

LXVI. POLICY:

A. This policy does not apply to matters that are of no reasonable concern to the Sheriff’s Office but does include personal communications with elected official about Sheriff’s Office business. It also does not apply to FOP correspondence between labor representatives and elected officials regarding legitimate labor concerns.

1. The Office of the Sheriff defines elected officials as federal, state, county or local legislative or elected officials, candidates, or their staff/representatives.

2. The Office of the Sheriff utilizes specific/official points of contact for communication with elected officials.

a. The Chief Financial Officer and/or Undersheriff are the official points of contact for the City Council.

b. The Chief Deputy, or in his/her absence, the Chief of Staff, is the point of contact for the Mayor’s Office and county, state, and federal elected officials.
3. Employees will forward requests from elected officials to the appropriate official points of contact.
   
a. If no official points of contacts available, the employee will contact the highest-ranking supervisor, who will contact the appropriate member identified in I-A. 

B. Employees will not communicate with elected officials regarding Sheriff’s Office-related matters. Instead, they will forward requests to the official Office of the Sheriff points of contact. 

C. The Office of the Sheriff points of contact will screen all outgoing Office of the Sheriff-related information with the Sheriff before releasing it to elected officials. 

   1. Exception: Sheriff’s Office employees who have regular interactions with elected officials about on-going issues may respond to such elected officials at the time of the request but must inform the Office of the Sheriff through their chain of command as soon as practical. 

   2. Exception: Personnel conducting community meetings may communicate with elected officials who are present, as appropriate, but must notify the Office of the Sheriff through their chain of command as soon as practical. 

LXVII. PROCEDURE: 

A. Employee 

   1. Receives an inquiry related to official Office of the Sheriff matters from an elected official or their representative. 

   2. Notifies their lieutenant/civilian manager via the chain of command. 

B. Lieutenant/Civilian Manager 

   1. Receives the notification and forwards any official request through the chain of command to the Office of the Sheriff point of contact (Chief Financial Officer or Undersheriff). 

C. Chief Financial Officer or Undersheriff. 

   1. Receives the notification and proposes a response. 

   2. Reviews the request and proposed response with the Sheriff, Chief Deputy, and Chief of Staff. 

384
3. Provides the appropriate (vetted) response to the elected official or representative under the FOP contract.
Director: Philadelphia Sheriff's Office

DIRECTIVE: #52
SUBJECT: PHILADELPHIA SHERIFF’S OFFICE-INJURY/EXPOSURE POLICY
ISSUE DATE: 05-14-2020
REVISED DATE: 02-23-2020

The City of Philadelphia’s Civil Service Regulation 32: Injury and Disability and the Pennsylvania Worker’s Compensation Act impose a duty upon the Philadelphia Sheriff’s Office to afford workplace injury benefits to all civil service employees.

The Sheriff’s Office endeavors to make certain all incidents of injury and exposures are properly investigated, and corrective measures taken to prevent future occurrences. The Office cannot meet the aim of reducing performance related injury or exposure incidents, without obliging that all Sheriff’s Office personnel report all incidents (including near misses) to their supervisor or unit commander regardless of severity or whether or not an injury occurred immediately, but no later than 24-hours after the incident.

POLICY:

1. Sworn Personnel who sustain an injury or exposure as a direct result of their job performance shall notify their immediate supervisor and submit an Employee Injury Report (82-S-58). In incidents involving sworn personnel, the employee shall also submit a Heart and Lung Claim Form (75-628). It should be noted that failure to do so may result in a denial of benefits under the provisions of the Civil service Regulations or the Pennsylvania Heart and Lung Claim Act (53 P.S. section 637).

2. All Sheriff’s Office employees who suffer service-connected injuries or exposures will be treated at an approved City Network Provider. Personnel who elect to receive treatment from a private physician or hospital will be responsible for any and all costs associated with such treatment. The only exception to this stipulation is instances where personnel are in severe medical emergencies and in order to prevent loss of life or serious disability, such staff are taken to the nearest medical facility.

3. A unit commander or supervisor once notified of an injury or exposure (no matter how minor) is to ensure that the employee prepares a Sheriff’s Office Incident Report, Employee Injury Report (82-S-58) and for sworn personnel, the Employee Injury Report
must be accompanied by Heart and Lung Form (75-628). This must be done even if the employee does not wish to seek immediate medical evaluation or treatment. The preparation and submission of the Employee Injury Report and Heart and Lung Claim Form is mandatory to ensure the Sheriff’s Office is in compliance to the Workmen’s Compensation Act and the Pennsylvania Heart and Lung Act. All questions concerning the Heart and Lung should be directed to Policy and Procedures or Human Resources.

4. The PA Heart and Lung Act only cover sworn personnel, who are injured in the course of duty and only those injuries of a temporary nature. Only sworn personnel will be required to prepare a Heart and Lung Claim Form. Determination of whether a service-connected injury is covered under the Heart and Lung Act will be made by the City Claims Administrator in consultation with Risk Management and Sheriff’s Office Internal Affairs Division.

5. Personnel complaining of dizziness, chest pains, light-headedness, etc., will be taken to the nearest hospital. Referrals will not be prepared for these types of complaints. When there is a question as to whether the illness is a duty related action, Human Resources will be contacted prior to issuing referrals.

**Treatment:**

1. Personnel injured or exposed to communicable diseases on duty will be sent or taken immediately after preparation of referrals, to one the City of Philadelphia Injury on Duty and Workers Compensation Providers clinics listed In Appendix “A”, except in serious emergencies. Personnel must at all times be treated within the City Network Provider to be eligible for Regulation 32 and Heart and Lung Benefits.

   A. Personnel complaining of an exposure due to contact with, or close proximity to, a potentially hazardous chemical will ensure this information is included in the Employee Injury Report. The unit commander will contact the Philadelphia Fire Department, if necessary, to ascertain the type of chemical involved for inclusion on the injury report. The unit commander will obtain the control number from the Fire Department for incidents where the Fire Department is called for chemical exposure.

2. The injured employee’s immediate supervisor will report this incident to the City’s third-party administrator, Comp services Inc. The report will be made via telephone at day or night, seven-days-a-week. The phone number for Comp services (1-866-463-2524). If no one answers the phone, a voice message relaying the specifics of the injury incident to the City’s third-party administrator. The supervisor or her/his relief will follow up with the City’s third-party’s administrator to ensure the injury report was received. This telephone report must be made immediately upon the injured employee’s first report of such claim to ensure coverage.

3. When the need arises for a Philadelphia County Deputy Sheriff to store service weapon(s) and/or privately owned weapon(s), while seeking treatment at any medical
facility within the City Network Providers for an on-duty injury, the following procedures are to be followed:

A. Upon reporting to the facility for initial or for follow up treatment, a deputy sheriff will request a lock box and a key from facility staff members, to lodge her/his weapon in secure fashion.
B. The deputy shall place her/his weapon(s) within the lock box.
C. The deputy shall maintain the key while at the facility.
D. The deputy shall upon completion of treatment, retrieve her/his weapon from the lock box.
E. The deputy shall return the key to a staff member of the City Network Provider.

4. All Sheriff’s personnel sustaining a human bite in the line of duty must inform the examining physician that the injury was the result of a human bite. Failure to do so may result in serious disability and the denial of benefits for the employee.

5. All orders and instructions concerning treatment procedures given by doctors at City Network Provider facilities shall be obeyed.

6. The Sheriff’s Office employee will be presented with two (2) copies of the “Encounter Forms” on each visit to a City Network Provider facility. One (1) copy will be retained by the employee and the other copy must be given to employee’s immediate supervisor, who in turn shall ensure the copy is delivered to Sheriff’s Office HR.

**Emergencies:**

1. In serious emergencies, the injured employee shall be taken to the nearest hospital or trauma center, when applicable, for First-Aid treatment and the following procedures shall be adhered to:

A. When an employee sustains an injury or an exposure, the employee’s immediate supervisor shall report all emergency treatment received by the employee as a result of the exposure and/or injuries suffered while on duty to the supervisor of Internal Affairs Division (215-686-3978) as soon as possible. The Chief Deputy and injured employee’s unit commander shall also be notified.

B. If the injured employee is to be transferred to another hospital, Barney 100 shall be notified prior to removal, if possible. Barney 100 supervisor shall immediately notify the Chief Deputy and Internal Affair Division of the transfer.

C. If the employee does not require further emergency treatment, she/he shall report directly to the appropriate City Network Provider (See Appendix “A”) with the completed Referral to City Network Provider (82-S-30) the next scheduled clinic day.

D. The employee’s unit commander shall notify the Sheriff’s Office HR on the first business day following emergency treatment. Memorandum and Incident Report shall be prepared and submitted through the appropriated channels to Sheriff’s Office HR
and Internal Affairs Division, whenever any Sheriff’s office personnel are admitted into a hospital. A copy of the memorandum shall be faxed immediately to HR.

**Reporting Injury:**

1. **Time limit for reporting injuries and/or exposures to the City Claim Administrator:**

   A. All Sheriff’s Office employees shall report to a City Network Provider for treatment within 48 hours after sustaining a service-connected injury or exposure.

   B. Employees who fail to report for treatment at the compensation clinic within the time allotted shall prepare a memorandum to her/his unit commander requesting an appointment to see Sheriff’s Office HR’s Safety Officer because of an on-duty injury. If the initial investigation by the unit commander reveals the employee’s claim to be reasonably valid the officer shall be sent to the HR Safety Officer who will issue a “Referral to City Network Provider” (82-S-30).

2. **Forms Required:**

   A. Referral to City Network Provider (82-S-30) – Original and three (3) copies.

      1. Each service injury or exposure shall be reported and approved on this form by the immediate supervisor on duty at the time of occurrence, prior to City Network Provider. (In case of an emergency, see subparagraph “C” of this section)

   2. **Distribution:**

      A) Original and copy –Taken by injured employee to treatment facility.
      B) Copy-Sent to HR Safety Officer with completed Employee Injury Report.
      C) Copy-Retained by employee’s unit commander.

   3. **Emergencies:**

      A) A Referral to city Network Provider (82-S-30) shall be prepared and approved by the immediate supervisor on duty when the injured employee is transferred from the emergency medical unit to a hospital contracted by the Risk Management Division of the Finance Department.

   B. **Employee Injury Report (82-S-58)-Five (5) Copies**

      1. All injuries or exposures on duty will be reported on this form within two (2) working days after occurrence by the injured employee (Type and ensure that all copies are clear). If the injured employee is hospitalized or unable, preparation of the form will be the responsibility of the first supervisor notified of the injury.

      2. A detailed explanation is necessary in Section II, block 31, to fully describe how the injury occurred, the particular body parts(s) injured etc.
3. When the injury is the result of a motor vehicle accident on duty, complete Part III of Employee Injury Report (82-S-58).

4. The unit commander and immediate supervisor will ensure that every block which applies is completed. The completion of Part IV (Evaluation) is particularly important. A check mark must be made which pinpoints any unsafe condition and/or unsafe act. In addition, any recommendation and/or action to be taken must be specific and not generalized. In addition, any recommendation and/or action to be taken must be specific and generalized. Incomplete injury reports shall be returned to the submitting unit commander for completion.

5. If the employee loses no time, specify at the upper right-hand corner of the Report.

6. Distribution:

   A) Original and two (2) copies-Safety Office
   B) Copy-Injured employee
   C) Copy-unit commander

C. Heart and Lung Claim Form (75-628) – Original and three (3) copies.

   1. Each service incurred injury or exposure to sworn officer shall be reported on this form.

   2. Distribution:

      A) Original and one (1) copy – HR Safety Officers
      B) Copy-Injured employee
      C) Copy-Internal Affairs Division

D. Memorandum (Employees claiming recurrence of service-connected injury)

   1. Any employee who claims the recurrence of a service-connected injury must obtain, from her/his unit commander, a memorandum which indicates that the employee may report to the HR Safety Officers. An incident report shall be forwarded to the Internal Affairs Division, citing the same.

   2. The HR Safety Officer will, if the circumstance warrants, refer the employee to appropriate City Network Provider.

**Responsibility for Investigation Service Connection of Injury:**

1. The unit commander shall investigate and make the initial determination as to the service connection of an on-duty injury or exposure claim by any Sheriff’s Office employee. The HR Safety Officer shall review the unit commander’s determination. The Sheriff or
her/his designee shall make the final determination as to the service connection of any off-duty injury.

2. An initial Referral to City Network Provider (82-S-30) shall be granted to the employee when there is an on-duty injury and there is a reasonable possibility of service connection to the injury. There shall be no presumption of service connection of cardiac or pulmonary cases, or injuries or exposure incurred coming to and from work.

3. Off-duty law enforcement action resulting in an injury shall be investigated by Internal Affairs. No referrals shall be issued until a determination is made by Internal Affairs to the deputy’s off-duty injury claim. This does not excuse the deputy from completing and submitting an Incident Report and an Employee Injury Report (82-S-58) to her/his unit commander, who will forward all documents to Internal Affairs. Internal Affairs shall forward its investigation report to the Chief Deputy, indicating its findings as to whether or not the deputy’s off-duty actions fall within Philadelphia Sheriff’s Office guidelines of law enforcement actions. If Internal Affairs finds the deputy’s actions are deemed to be enforcement of law and the Chief Deputy approves of their determination, then the matter shall be forwarded to the Sheriff for final approval. Once approved by the Sheriff, the HR Safety Officer shall issue a “Referral to City Network Provider” (82-S-30).

A. Deputies involved in an off-duty incident, who are claiming the incident was a law enforcement action and who have been injured as a result of that action will be carried as “Sick” on the Daily Attendance Report. Such deputies shall remain in “Sick” status until a determination is made in favor of their off-duty claim or until they are cleared to return to work by Employee Medical Services, 1901 Fairmount Avenue.

B. Deputies who are returned to work by Employee Medical Services before the completion of Internal Affairs’ investigation may request a change of status of the days missed because of off-duty injury. To do so, deputies through the chain of command must submit a memorandum to the Chief Deputy. The Chief Deputy will review the case and give a disposition.

**Service-Connected Disability:**

1. Determination as to whether or not a disability is service connected will be made on the basis of the following:

   A. The Employee Injury Report
   B. The Sheriff’s Office Incident Report, the incidents report of Sheriff’s Office employee, statements from non-Sheriff’s Office witnesses and responders.
   C. The findings of the doctors at the City Network Provider.
   D. Evidence which the employee may possess (private medical records) concerning employees’ claim of service-related injury/illness. These records shall be submitted at the employee’s own expense to HR. HR shall forward these records to City Network and obtain a receipt.
E. Any other relevant evidence pertaining to the employee’s claim of service-related injury.

**Responsibilities-No-Duty/Limited Duty Status Personnel:**

1. Employees injured or exposed on-duty and placed on No-Duty/Limited Duty shall:

   A. Be prohibited from engaging in outside employment.

   B. When leaving their residence for extended periods of time (weekends, weeks, etc.) notify their unit commanders of their destination, date and time of departure and expected date and time of their return. Such employees shall provide their unit commanders with a phone number where they can be reached. This only applies to No-Duty Status personnel.

1. The unit commander shall submit this information to HR and Internal Affairs. Both units shall place the information in the file of the employee.

**Duty Status:**

1. The duty status of an employee with a service-related disability will be determined only by the doctors at the City Network Provider (new injuries and reoccurrence). Employees sustaining an on-duty injury are not required to report to Employee Medical Services at 1901 Fairmount Avenue. It is the employee’s responsibility to notify their duty status to her/his unit commander, who will forward this information to HR. The categories of duty status are as follows:

   A. No-Duty – Employees will be carried as “I” (Injured ON-Duty) on the Daily Attendance Report by their immediate supervisor. If the service connection has not been determined, the employee will be required to use, sick, holiday, vacation, and compensatory time. (if later determined to be service related, such time will be converted to “I” time.

   B. Limited Duty – An employee placed on Limited Duty status shall report to her/his Deputy Chief for assignment. An employee re-assigned due to Limited Duty Status will report to the unit assigned to her/him by the Deputy Chief. The deputy’s unit commander shall ensure that she/he is carried “D” (Detailed) on her/his normal Daily Attendance Report. The employees who remain assigned to their own units shall be carried on the Daily Attendance Report as if they were working full duty, through the other column will be “LD” (Limited Duty).

1. The Deputy Chief shall:

   A) Assign an injured employee to their current assignment for the first 30 days of limited duty status.
B) After the 20th day, if the limited duty status is to continue beyond 30 days, the Deputy Chief shall confer with the remaining Deputy Chief to determine where the employee best serves the need of the office.

2. Active Duty – An employee who has been treated for an on-duty injury or exposure and returned to active duty.

NOTE: If after returning to active duty an employee claims a reoccurrence, the procedures outlined in the Article entitled; Reporting Injury, section 2 must be followed.

2. All changes to the duty status of employees will be indicated in the OnePhilly Computer System. (This does not relieve the employee from the responsibility of notifying her/his unit commander of her/his duty status).

3. An employee who is placed on active duty or limited duty by the City network Provider but fails to report to work because of their condition shall be considered insubordinate and will not be carried as “I” (Injured On-Duty) on the daily Attendance Report. The employee will be carried as Holiday, Vacation, or Compensatory Time, until an appeal is filed with the Civil Service Commission. Once filed, a date stamped copy of the appeal will be submitted to the employee’s unit commander, at which time the unit commander shall permit the use of sick time, subject to the provision of the Civil Service Regulations. The unit commander shall ensure that a copy is immediately forwarded to and received by the HR Safety Officer.

4. An employee carried under the Heart and Lung Act, who is placed on Active or limited Duty by the City Network Provider but fails to report to work, the Undersheriff shall file a Petition to Terminate, modify or Suspend benefits under the Heart and Lung Act to the Heart and Lung Arbitration Panel. The employee shall continue to remain in the previous status mandated by the City Network Provider until the final determination is made by the Heart and Lung Arbitration Panel.

5. Determination as to whether or not a disability has developed into a state of permanent and partial or total disability is based on the following:

A. Decision of the Medical Director, City of Philadelphia.
B. Decision of the Sheriff.
C. For Heart and Lung cases, the decision by the Heart and Lung Arbitration Panel.

6. Any employee assigned to limited duty and who is undergoing physiotherapy prescribed by a physician of the City Employee’s Compensation Clinic or any other facility under contract to provide such service shall:

A. Be permitted a sufficient amount of time to travel from place of assignment to the facility where the therapy is to take place and an equally sufficient amount of time to return to place of assignment upon completion.
B. Not be carried on the Daily Attendance Reports as “working” during the period of absence from her/his limited duty assignment.

C. Be carried on the Daily Attendance Report as Injured-On-Duty, “I” to the nearest one-half (1/2) hour during such absences.

D. Report on and off duty to the unit commander at her/his limited duty assignment. The unit commander shall ensure that the actual time of departure and return is recorded on the Daily Attendance Report

1. Overtime is not authorized for limited duty personnel. Therefore, if reporting for duty before proceeding to the medical facility or returning afterward places the employee in an overtime situation, the employee shall be permitted to report on or off duty by telephone to the unit commander at her/his limited duty assignment.

7. Any officer, regardless of rank, who is placed in Injured Duty (IOD) status for more than one (1) working day shall be immediately assigned to an area within the Sheriff’s Office, where there is limited contact with the public.

BY ORDER OF:

[Signature]

SHERIFF DATE

394
A. **POLICY:**

1. This policy applies to all Philadelphia Office of the Sheriff employees.

2. Sheriff’s Office employees follow a structured chain of command.

3. All Philadelphia Sheriff’s Office employees are subordinate to the Philadelphia Sheriff. Employees are subordinate to all ranks above their position.

4. The Philadelphia Sheriff’s Office chain of command applies while on duty or off duty (law enforcement actions/contacts).

5. Sworn employees are ranked:

   a. Philadelphia Sheriff

      1) The Sheriff is the overall commander of the Office of the Sheriff.

   b. Chief Deputy Sheriff

      1) The Chief Deputy is 2nd in Command of all Operations within the Office of the Sheriff and serves as the Chief Administrative Deputy to the Sheriff.

      2) Assists in establishing office policies.

      3) Directs the administrative functions of the office as carried out by all units under his/her command.
4) Conducts staff conferences, inspections, and surveys to determine office needs and evaluate overall activities and operations.

c. Undersheriff

1) Serves as the primary legal counsel to the Office of the Sheriff, within the scope of duties performed.

2) Interprets and advises the Sheriff and Sheriff's personnel on matters of law and court procedures.

3) Makes legal decisions and determinations on matters relative to his/her office, legal transactions relating to properties, schedules of payments, purchasing agreements, etc.

4) Assists in establishing office policies.

5) Performs other related duties as required.

d. Chief of Staff

1) The Chief of Staff manages Sheriff's Office facilities, the Public Information Office, Community Programs, and the Human Resources Department.

e. Deputy Chief, Chief Inspector, and Inspector: In chain of command order-Deputy Chiefs, Chief Inspectors and Inspectors are civil service employees appointed by the Sheriff, empowered to serve in command capacities over bureaus.

f. Captain: command sections; a division of a bureau.

g. Lieutenants: command units; a section of a division or squad. Several units may work within one shift.

h. Sergeants command shift: sergeants may also command a detail, which is a subdivision of a squad or sector assigned a specific task.

i. Deputy Sheriff Officer: Deputies work within a shift on special assignments, tactical, or security related posts and patrols.

j. Deputy Sheriff: Deputies, who serve legal process, enforce court orders, injunctions and judgments and conduct sales of real and personal property.

k. Non-sworn employees are ranked under their collective bargaining agreements.
6. The Office of the Sheriff follows a succession of command in the unlikely event the Sheriff is incapacitated. The Office of the Sheriff command succession is:

1. Chief Deputy Sheriff
2. Undersheriff
3. Chief of Staff
4. Deputy Chief, Uniformed Services Division
5. Deputy Chief, Internal Affairs
6. Deputy Chief, Training
7. Chief Inspector, Real Estate

B. PROCEDURE:

1. Sworn Employees shall assume command during operational situations until a higher ranked supervisor relieves them.

   a. Sworn employees responding to an operational situation will follow the command of a higher-ranking employee and abide by the Incident Command Systems.

   b. The physical presence of a higher ranking sworn employee at an operational scene indicates no immediate assumption of command and decision-making responsibilities.

   c. Employees may delegate duties to their subordinates.

   d. An employee may assign a subordinate employee the same authority and responsibility they possess to accomplish a specific task. The delegating employee remains responsible to complete the delegated task.

2. Office of the Sheriff employees shall train their subordinates.

   a. Employees in a supervisory role will provide training for their subordinate employees.

   b. Subordinate employees will report the need for training to their supervisors.

   c. Employees in a supervisory role will train their subordinate employees in the duties of that role if the supervisor cannot perform their duties.

8. Supervisors shall attend supervisory development training

   a. Deputy Chiefs will send deputies to supervisory development training for all subordinates’ assignments within 90 days of promotion to higher rank.
9. Command level employees take responsibility for every aspect of their commands:
   
a. Employees serving in a supervisory role will coordinate and direct subordinates and allocate resources to achieve the operations objective.

b. Employees in a supervisory role will perform the full range of administrative functions relying upon policy, direction, training, and personal initiative as a guide for themselves and their command in achieving the highest level of performance possible.

10. Employees shall communicate through the chain of command:
   
a. Where otherwise provided in this Manual, or where the information is sensitive and requires communication outside the chain of command, an employee may communicate directly with any higher-ranking employee.

b. The higher-ranking employee is then responsible for taking immediate action where appropriate and informing the next level up in the chain of command of the information.

11. Employees shall communicate through the chain of command:
   
c. Where otherwise provided in this Manual, or where the information is sensitive and requires communication outside the chain of command, an employee may communicate directly with any higher-ranking employee.

d. The higher-ranking employee is then responsible for taking immediate action where appropriate and informing the next level up in the chain of command of the information.

BY ORDER OF:

[Signature]

SHERIFF DATE

398
DIRECTIVE: #54
SUBJECT: WRITTEN DIRECTIVES
ISSUE DATE: 04-20-2020
REVISED DATE: 01-04-2021

C. POLICY:

A. Directives: for the purpose of this directive shall encompass all Policies, Procedures, Directives, Rules, Special Orders, Special Operations Procedures, Divisional Memorandums, Orders, etc.

1. When initiating a new directive, persons requesting the order shall first obtain approval through their chain of command then submit a draft proposal of the order to the Deputy Chief of Policies and Procedures. The Policies and Procedures Division shall be responsible for research, development, staff review and, upon approval of the Sheriff, Chief Deputy, and Undersheriff, for distribution and publication as a Directive. All Directives shall require all employees’ electronic documentation of receipt and a passing test score in policy management software.

2. Directives will be issued, modified, or withdrawn only by the Sheriff. All requests for amending a directive shall follow the procedures in this directive. The authority of a person to rescind or amend a bureau directive/unit is restricted to those orders that the person is authorized to issue.

3. Definitions

   a. Revisions - Refers to replacing an existing directive or a portion thereof with a revised order or the insertion of a new procedure into the Directives Manual.

   b. Rescindments - Refers only to the removal of a procedure from the Directives Manual or the cancellation of any Special Order, SOP, etc.

   c. Mandatory and Permissive verb forms
1) The words "shall" "will" and "must" and "ensure" are mandatory in intent.
2) The word "may" is permissive in intent.
3) The word "should" is advisory in intent.

4. Directive Manual - Refers to the complete document containing all directives with table of contents and index in tangible copy and maintained electronically (in policy management software), distributed as either hard copy, electronic copy posted on the internal Office of the Sheriff website or distributed in another medium authorized by the Sheriff (i.e., USB, flash drive, portable drive, or other electronic methods as future technology may dictate).

B. Memorandums/Inter-office correspondence

1. Memos/Inter-office correspondence orders shall be amended, rescinded, or revised with the issuance of a new memo/inter-office correspondence which shall delineate the changes, including self-canceling provisions, if applicable.

2. The Directive Manual shall be reviewed annually and updated as necessary by the Policy and Procedures Unit.

C. Special Orders

1. When necessity requires the establishment of a Sheriff’s Office Special Order prior to advancement to a Directive, persons generating the procedure shall follow the same process as a Directive. All Special Orders shall require an employee’s documentation of receipt (IA-1).

D. Memorandums or divisional/bureau directive

1. When necessity requires establishing a guideline or procedure to be followed for personnel below the Office level, the authorized person shall forward the proposed directive to the Deputy Chief, Training, Deputy Chief, IAD, and Undersheriff, for a comprehensive review of the document for conflicts with directives, other policies, law, or contracts.

2. If the directive conflicts or violates existing procedures, it shall be returned to the submitting party within seven (7) business days, noting the areas requiring change highlighted. If no changes are necessary, it shall be signed by the Deputy Chief of the Policy and Procedures Unit, Deputy Chief of IAD, and Undersheriff acknowledging their review and returned noting that no conflicts exist.

3. Directives created in this category shall be furnished to employees within the bureau with the same required documentation of receipt (IA-1) in policy management software.
E. Standard Operating Procedures (SOPs)

1. Standard Operating Procedures (SOPs) will be developed by the unit, section, division, or bureau, and forwarded to the Deputy Chief of Policy and Procedures for review for conflicts with other written directives, laws, and contracts. Once returned to the creator/author by the Policy and Procedures Deputy Chief, the SOP will be approved through the submitting party's chain of command. SOPs should be reviewed annually by the affected unit, section, division, or bureau.

2. All SOPs will include sections on statement of purpose; organization; personnel duties, authority, and responsibilities; operations; and any other areas as determined by the respective Deputy Chief.

3. All SOPs shall be retained in policy management software. Any revision to SOPs by the issuing organizational segment shall be submitted to the Deputy Chief of Policy and Procedures, Undersheriff, and Internal Affairs prior to utilization.

4. SOPs shall be furnished to all employees within the unit, section, or division with a required documentation of receipt and training retained in policy management software.

D. DISTRIBUTION:

A. Distribution of approved Directives shall be the responsibility of the Policy and Procedure Unit and shall be based on the most effective method available.

B. Upon employment, all sworn personnel are issued an email address and policy management software access to a Directives Manual and shall be responsible for understanding and practicing updates to the manual; all civilian employees shall be provided redacted access to directives via policy management software.

C. All employees shall demonstrate they have received and understand the orders through electronic signature and by-passing examinations based upon the contents of any new or changed directive(s).

D. Employees shall receive training from the Training Division while “on-boarding” with Human Resources on how to access and utilize the policy management software.

E. Accountability for compliance with all orders rests with the employee AND his/her direct supervisor.

F. Distribution of General Orders and Special Orders.
1. Upon the issuance of a new directive, the Deputy Chief of Policy and Procedures will notify all employees.

2. The division Deputy Chief/Civilian Manager or designee shall be responsible for ensuring that each employee acknowledges receipt by completing policy management documentation and testing. The maintenance of electronic documentation of receipt will be the responsibility of the Deputy Chief of the Policy and Procedures Unit.

3. If applicable, no later than ten (10) business days after the order is issued, the division commander/manager is responsible for returning any hard copy sign-back sheets to the Policy and Procedures Unit, which shall maintain a hard-copy file of these forms.

4. The Deputy Chief of Policy and Procedures shall ensure all directives are redacted for sensitive information and posted publicly on the PSO website in a timely manner.

E. CONTROL OF DIRECTIVES:

A. The Policy and Procedures Unit shall maintain a master file of all Directives, General Orders, Special Orders, Bureau Directives, and Standard Operating procedures.

B. The Undersheriff and IAD Deputy Chief shall be responsible for ensuring the orders comply with State and Federal laws and shall maintain a master file of all Personnel Orders.

C. All Captains shall maintain a master file of all Standard Operating Procedures and all directives, including Training and Procedural Directives, issued within their areas.

BY ORDER OF:

[Signature]

SHERIFF DATE
DIRECTIVE: #55
SUBJECT: DISCIPLINARY PROCEDURES
ISSUE DATE: 03-18-2020
REVISED DATE: 02-08-2021

LXVIII. PURPOSE:

A. This Directive establishes standardized disciplinary guidelines for the process used to investigate and process Sheriff’s Office complaints and grievances.

B. This policy provides the philosophy for employee conduct and professionalism. It is not the Sheriff’s Office intent to interfere with or constrain the freedoms, privacy, and liberties of employees; discipline will only be imposed where there is a connection between the conduct and the duties, rank, assignment, or responsibilities of the employee. The Sheriff’s Office expects all employees to treat all people with dignity; remember that community care-taking is at times the focus, not always command and control; and that the guiding principle is to treat everyone with respect and courtesy, guarding against employing an officious or overbearing attitude and refraining from language, demeanor, and actions that may cause the individual feeling belittled, ridiculed, or intimidated.

C. This section applies to all Sheriff’s Office employees. The content is not all-inclusive. Employees must also comply with conduct expectations in other manual sections pertaining to them.

LXIX. SCOPE:

A. All Office employees shall be subject to disciplinary action for acts of misconduct.

B. In reference to civil service employees, misconduct is defined as any act committed or omitted as required by the twelve (12) rules listed in this directive.

1. The form of disciplinary action for civil service employees may be:
a. Counseling Memo.
b. Written reprimand.
c. Suspension without pay.
d. Demotion.
e. Indefinite suspension without pay.
f. Dismissal.
g. Automatic 30-Days w/intent to dismiss in cases involving any felony offense conviction.

2. The following twelve (12) rules are examples of causes for disciplinary action, including removal or suspension for civil service employees.

a. Conviction of a felony or other crime involving moral turpitude.
   i. Conviction of a felony is cause for dismissal and conviction of a M1 or M2 may be cause for disciplinary action or indefinite suspension.

b. Violation of the provisions of the FBI CJIS or City of Philadelphia IT policy.


d. Neglect of duty.

e. Discourtesy to the public or to fellow employee while the deputy is in the line of duty.

f. Acts showing lack of good moral character.

g. Drinking intoxicants while on-duty.

h. Conduct Unbecoming or behaviors prejudicial to good order.

i. Absence without leave.

j. Shirking duty or cowardice.

k. Violation of any of the rules, regulations, or any orders of the Office of the Sheriff.

3. Disciplinary procedures for non-civil service personnel are governed by the City of Philadelphia Rules and Regulations.

4. Each deputy chief shall ensure that all sworn and civilian employees in their divisions and/or sections have a copy of the City of Philadelphia Rules and
Regulations and the Deputy Chief of Policy and Procedures will ensure that it, and all directives, are maintained to a current status using policy management software.

C. Disciplinary action for non-civil service (exempt or non-exempt) employees is normally applied in progressive steps when documented performance is unsatisfactory. The form of disciplinary action may be:

1. Oral warning.
2. Written warning.
3. Disciplinary probation period.
4. Reduction in pay rate.
5. Suspension.
6. Demotion.
7. Dismissal.

D. Prior to initiating disciplinary action involving non-civil service personnel, the supervisor initiating the process shall consult the appropriate section of the City of Philadelphia Rules and Regulations.

1. The supervisor shall also consult with the Undersheriff and appropriate Human Resources Staff as assigned by the Undersheriff prior to finalizing any disciplinary action other than an oral or written warning.

E. Emergency Disciplinary Action: Non-Civil Service Personnel

1. If the actions of a non-civil service employee necessitate immediate disciplinary action and the Undersheriff is unavailable, the supervisor shall adhere to the following procedures:

   a. Instruct the employee to leave the work site at once and to report back to work either the next day or at a time specified by the supervisor.
   b. Prepare a written report detailing the circumstances leading to the action taken and submit the report to the employee’s division deputy chief or equivalent civilian director.
   c. At the earliest opportunity, consult with the Undersheriff and HR Director.

2. Subsequent to the above steps, the normal procedures outlined in the City of Philadelphia Rules and Regulations, shall be followed.

F. Appeals and Grievances: Non-Civil Service Personnel

1. The appeal and grievance processes for non-civil service employees are detailed in the City of Philadelphia Rules and Regulations. Oral warnings, including documented oral warnings, are not subject to grievance. The City of Philadelphia
Rules and Regulations must be made available to any non-civil service employee requesting access to these items.

**LXX. PERSONNEL COMPLAINTS:**

A. A personnel complaint is an allegation, received from any source, of misconduct by an Office employee.

B. All personnel complaints shall be accepted, and a Personnel Complaint form shall be completed without unnecessary delay whenever:

   1. The complaint is of misconduct of any nature.

   2. The complaint is received from a source outside the Sheriff’s Office or the alleged violation involves a Sheriff’s Office employee.

C. When any employee becomes aware that a person wishes to make a complaint against a Sheriff’s Office employee, the employee will immediately notify a supervisor who shall report to that location and receive the complaint.

D. Whenever an employee who is not a supervisor becomes aware, either through personal observation or other means, of possible misconduct they shall, if applicable, take corrective action to preclude continuation or escalation of the incident and shall immediately notify a supervisor (i.e., a deputy using excessive force).

E. When any supervisor becomes aware of possible misconduct, either through personal observation or other means, the supervisor shall immediately act to prevent continuation or aggravation of the incident. The supervisor shall also conduct a preliminary investigation, which shall include, when applicable:

   1. Names, identification numbers, and assignments of all involved employees, including employees who are witnesses.

   2. Names, addresses and telephone numbers of the complaining person and any known witnesses to the incident who are not Office employees. Times, locations, and business and residential telephone numbers where these individuals may be contacted shall be indicated.

   3. A statement from the complaining person obtained by an interview of that person by the reporting supervisor.

   4. Photographs of actual or claimed injuries to the complaining person. Photographs shall be taken in all cases involving allegations of excessive force.
5. Any available information regarding medical treatment obtained by the complaining person as a result of the incident.

6. The disposition of any evidence obtained.

7. A supervisor shall not be assigned to investigate alleged misconduct if they are the reporting party, the ultimate decision-maker regarding disciplinary action, or if they have any personal involvement regarding the alleged misconduct.

   a. When warranted, the allegation of misconduct shall be reported on a Personnel Complaint form.

      1) Signature of the reporting party, if possible.
      2) If the reporting party refuses to sign the form or cannot sign the form for a compelling reason, such as incapacity or the person lives a considerable distance outside the city, the interviewing supervisor shall include the reason for not obtaining the signature in the narrative portion of the form. In instances where a valid reason exists for not obtaining the reporting party’s signature, the signature of the interviewing supervisor in the “Reporting Party” block will be considered a valid substitute for the signature of the reporting party.
      3) If the supervisor becomes aware of the misconduct through personal observation or the misconduct is of a nature whereby the complaining party is the administrative entity of the Office, the reporting supervisor shall sign the Personnel Complaint form as the “Reporting Party.”
      4) The supervisor may be asked to elevate the complaint to a higher-level supervisor within the chain of command. If that request is made, and a higher-level supervisor is working, the higher-level supervisor from that location or any other location working will be summoned to the scene.

   b. Information on witnesses who are not Office employees and investigative results, other than the reporting party’s statement, shall not be included in the Personnel Complaint form. Such information shall be documented in a separate memorandum and directed to the Internal Affairs Division.

   c. The reporting supervisor shall forward the completed Personnel Complaint form in the following manner:

      1) The original copy shall be sent to the Internal Affairs Division via electronic incident report management system, if possible.
      2) A copy shall be sent to the involved employee’s captain.
      3) A copy shall be provided to the involved employee’s deputy chief.
F. The commander of the Internal Affairs Division shall ensure the assignment of a permanent investigation number to a received Personnel Complaint form and shall provide the number to the involved employee's division Deputy Chief.

G. Minor incidents which will not reflect discredit upon the Sheriff's Office, but which indicate a need for some form of corrective action and/or training (any offense that could incur a maximum of one day or below with aggravating circumstances factored), may be dealt with by the involved employee's immediate supervisor with the review and concurrence of the involved employee's Captain.

H. The Personnel Complaint form shall not be completed when complaints are solely against Office policies or procedures. If a complaint is determined to be concerning Office policies or procedures and no misconduct is indicated, and the incident cannot be explained to the complaining person's satisfaction, that person shall be referred to the organizational entity having administrative control over the subject matter.

I. Complaints from Intoxicated Persons or a Third-Party Source.

1. When a personnel complaint is received from an intoxicated person, a Personnel Complaint form shall be prepared and processed, without the complaining person's signature. The complaining person shall be re-interviewed at the earliest opportunity after having regained sobriety by the supervisor assigned the investigation. During the re-interview, the complaining person shall be asked to sign the Personnel Complaint form. Refusal to sign the form will not invalidate the complaint process.

2. When a personnel complaint is received from a third-party source, a complaint form shall be prepared and processed. The third-party source shall be asked to sign the Personnel Complaint form as the reporting party.

3. In either event, unless the personnel complaint is validated by subsequent interview of the intoxicated person or an actual party to the incident, the final disposition of such complaint shall not be listed on a deputy's Internal Affairs Division record. All reports related to such complaints shall be filed as miscellaneous memorandums by the Internal Affairs Division.

J. The personnel complaint form shall be completed on personnel complaints received from anonymous sources; however, when information is received by a supervisor which originated from an anonymous source, the supervisor shall submit the anonymous complaint via memorandum, detailing the information received, and forward it to the Internal Affairs Division.
1. If the information received is of a nature that would jeopardize the integrity of an investigation by being reduced to writing, it shall be communicated via telephone to the Deputy Chief of Internal Affairs or Undersheriff via telephone.

2. If the information received describes misconduct of a nature which, if true, would normally result in a form of disciplinary action in excess of 1-day suspension or more, a preliminary investigation will be conducted.

3. When warranted, the allegation of misconduct shall be reported on a Personnel Complaint form. If the identity of the anonymous reporting party cannot be determined or if identified, refuses to sign the Personnel Complaint form, the signature of the investigating supervisor in the “complainant” block will be considered a valid substitute for the signature of a reporting party.

LXXI. DISCIPLINARY PROCEDURES: SENSITIVE INVESTIGATION

A. When a personnel complaint or incident is of a nature that the integrity of the investigation may be compromised or jeopardized by reducing the incident to writing, the reporting supervisor shall immediately report the incident to their commander, who shall report said incident to the Deputy Chief Internal Affairs Division.

B. If the reporting supervisor has reason to believe the integrity of the investigation may be compromised by passage through normal channels, the supervisor shall personally report the incident directly to the Deputy Chief Internal Affairs Division.

C. When immediate action is required or the seriousness of the incident is such that it may subject the Office to severe criticism or liability, the reporting supervisor shall provide immediate notification to the involved employee’s division commander and to the Deputy Chief Internal Affairs Division.

1. In incidents of this magnitude, division Deputy Chiefs may temporarily relieve the involved employee from duty, with pay, and shall, when applicable, take custody of a deputy’s badge, identification card, and service weapon.

LXXII. DISCIPLINARY PROCEDURES: SUPERVISOR RESPONSIBILITY

A. Supervisors/Captains who become aware of alleged misconduct shall:

1. Ensure that a Personnel Complaint form is prepared without unnecessary delay and signed by the interviewing supervisor and the reporting party.

2. Ensure that an appropriate preliminary investigation has been completed.
3. Ensure that all complaint forms, copies, and related reports are forwarded to the appropriate personnel as described in this directive and that all notifications required are completed.

4. The investigator or supervisor performing the investigation shall provide the employee with the written allegations in the complaint no less than 48 hours before the initial interview or requesting any memorandum or other correspondence related to the incident from the employee.

NOTE: The 48-hour notice does not apply to on-scene investigations that occur immediately after an incident.

B. Deputy Chiefs have the primary responsibility for investigating personnel complaints made against employees of their commands. A Deputy Chief who becomes cognizant of any allegation of misconduct shall monitor all resulting activities and shall ensure that personnel under their command have fulfilled their responsibilities provided in this order. A deputy chief may request that the Internal Affairs Division conduct an investigation on any allegation of misconduct or personnel complaint.

LXXIII. DISCIPLINARY PROCEDURES: INTERNAL AFFAIRS DIVISION RESPONSIBILITIES

A. The Deputy Chief of the Internal Affairs Division shall act in a staff advisory capacity when necessary. The deputy chief may assume responsibility for the investigation of any personnel complaint when, in the opinion of the deputy chief, it is advisable to do so.

B. The Internal Affairs Division shall assume responsibility for a personnel complaint when:

1. It has been alleged an employee has committed any felony or Class A or B misdemeanor.

2. The allegation of misconduct is against employees of more than one division.

3. The investigation involves an allegation of:
   
   a. Excessive force,
   b. Sexual harassment,
   c. Hostile work environment,
   d. Disparate treatment due to gender, race, ethnicity, age, or sexual orientation,
   e. Retaliation for reporting the misconduct of another,
   f. Inappropriate conduct or comment of a sexual nature, or
   g. Inappropriate comment regarding gender, race, ethnicity, age, or sexual orientation.
C. The Deputy Chief-Internal Affairs Division has the authority to obtain the advice and assistance of any departmental entity.

D. In the event an Assigned Investigator is unable to contact a complainant or witness for interview (or follow-up investigative statements) the Deputy Chief of Internal Affairs will ensure the Assigned Investigator exercises due diligence to contact the complainant or witness. Due diligence shall include at least two visits to the last known address of a complainant/witness and mailing a certified letter with delivery confirmation via USPS. Every contact attempt will be separately logged into the IAD electronic file management system.

LXXIV. ARRESTED SHERIFF’S OFFICE EMPLOYEE

A. If an employee of the Office is detained or arrested for any criminal offense within the City of Philadelphia, the deputy detaining or arresting the employee shall immediately notify a supervisor of the division/jurisdiction in which the employee is detained or arrested.

B. A supervisor who has been notified that an employee of the department has been arrested or detained shall immediately proceed to the scene and shall ensure that the Deputy Chief-Uniform Services is immediately notified.

C. The Deputy Chief-Uniform Services shall ensure immediate notification is made to:

1. The Internal Affairs Division Deputy Chief.
2. The Deputy Chief of the employee’s division of assignment.
3. The employee’s Captain or director.
4. The Public Information Deputy.

D. When a need is indicated to present to the jail an employee who has been arrested, the Deputy Chief-Internal Affairs shall contact the involved employee’s bureau Deputy Chief or assistant department head for booking approval. If the involved employee’s Deputy Chief or assistant department head is unavailable, the duty Deputy Chief shall be contacted for booking approval.

E. The employee’s bureau Deputy Chief and Undersheriff shall determine if the employee is to be presented to the appropriate jurisdiction jail for booking.

F. If no deputy chief is available, the Deputy Chief of Internal Affairs Division and the Undersheriff shall make the determination as to whether booking shall take place.

G. The Internal Affairs Division or the appropriate specialized investigative unit shall investigate whenever an employee is arrested for or believed to be a principal suspect in a felony or M1 or M2 offense. When applicable, they shall be responsible for submitting the criminal case to the District Attorney for consideration of criminal
prosecution. The Deputy Chief-Internal Affairs Division has the discretion to assume responsibility for investigations related to class M1 violations.

H. When any employee of the Office is detained or becomes aware that they are believed to be the principal suspect in a criminal offense, other than minor traffic violations committed outside the City of Philadelphia, the employee shall as soon as possible notify a on call, or on-duty supervisor.

I. When any employee of the Office is detained or becomes aware that they are believed to be the principal suspect in a criminal offense, other than minor traffic violations committed outside the City of Philadelphia, the employee shall as soon as possible notify a on call, or on-duty supervisor.

J. Any supervisor who is notified regarding the detention or arrest of an employee by another law enforcement agency, other than minor traffic violations, shall ensure that immediate notification is made to the Internal Affairs Division and to the applicable Divisional Deputy Chief of the involved employee.

K. The on-call or working Internal Affairs Division investigator shall respond to the scene or to the indicated outside agency (within a 3-hour radius) when the incident involves an alleged felony, M1, or M2 violations.

1. A supervisor from the involved employee's division of assignment shall respond on alleged class C misdemeanor violations if the violation is of a magnitude to require immediate investigation and is within a 1-hr radius.

   a. Regardless of whether a supervisor responds to the scene, a Personnel Complaint form shall still be prepared and processed.

2. The responding supervisor shall conduct a preliminary investigation and a Personnel Complaint form shall be prepared, processed, and added to the Sheriff's Office.

3. The responding supervisor shall advise concerned members of the outside agency that the preliminary investigation is for internal administrative purposes only and that any evidence obtained by the responding supervisor solely as a result of interviewing the involved employee shall not be disclosed to the agency conducting the criminal investigation. Responding supervisors shall exercise extreme care not to interfere with the investigation of the outside agency.

LXXV. DISPOSITION OF ADMINISTRATIVE INVESTIGATIONS
A. Administrative investigations which may result in disciplinary action, whether conducted by the Internal Affairs Division or the involved employee’s division of assignment, shall be completed within ninety (90) calendar days from the date the complaint is received or initiated.

NOTE: Due to the complicated nature of some investigations, the investigation deadline may be waived by the division Deputy Chief or Undersheriff but will not exceed 179 days.

B. Unless approved by the Sheriff or designee, a recommendation of potential charges (if warranted) is the responsibility of the division investigating the incident.

C. If the incident is minor, as described in this directive, the complete administrative investigation prior to the issuance of any discipline will be the responsibility of the chain of command of the deputy at the time of the incident or misconduct. If an employee is transferred/moved prior to the completion of the investigation, the chain-of-command responsible for that employee at the time the incident occurred will continue the investigation, review, and notifications. Reassignment of the deputy does not reassign responsibility of any part of the investigative, notification or discipline process.

D. If the incident or offense is investigated by the Internal Affairs Division, the complete administrative investigation AND recommendation for subsequent action will be made by the Internal Affairs Investigator.

E. The assessment of investigations and their findings by the chain of command or the IAD Investigator, including letters of transmittal or files via electronic file management system, shall be completed within fifteen (15) calendar days of the date the investigation is completed or the date the investigative report is received from the Internal Affairs Division.

F. A completed investigation shall be submitted to the involved employee’s division Deputy Chief by the supervisor of same through the chain of command via electronic file management system and shall include a summary of facts prepared by the employee’s Captain with an appropriate conclusion, classifying each specific act of misconduct into one of the following categories:

1. **Unfounded:** The investigation reveals sufficient evidence to believe the complained of act did not occur.

2. **Exonerated:** The investigation reveals the complained of act occurred but was legal, proper, and justified.
3. **Not Sustained:** The investigation discloses insufficient evidence to believe
the complained of act either did or did not occur.

4. **Sustained:** The investigation discloses evidence that is sufficient to conclude
the complained of act occurred.

G. When an investigation subsequently discloses additional allegations of misconduct
which were not described in the original personnel complaint and the classification of
the original complaint is other than sustained, a new complaint form shall be
prepared, and a supplemental investigative report completed. When any allegation of
misconduct in the original personnel complaint is sustained, the new allegations may
be recorded as separate supplemental charges in the investigative report for the
original complaint.

H. If any allegation of misconduct is sustained, the employee's first-line supervisor at the
time the incident occurred shall:

1. Prepare the summary report.

2. Discuss the summary report with the applicable chain of command, i.e.,
sergeant will discuss the complaint with the lieutenant and captain and
enter a collective recommendation for disciplinary action.
   a. The recommendation should be within disciplinary matrix guidelines
      and should factor the severity of the offense and any aggravating
      factors if they exist.
   b. The deputy's personnel record should also be used in making a
decision, concerning discipline.
   c. Discuss the findings and recommendation for disciplinary action with
      the involved employee in person, documenting the meeting in the
      summary report.

3. Forward the completed investigation and summary report for review by the
remaining layers of the employee's chain of command via Sheriff's Office
electronic case management system.
   a. If the finding is a result of a criminal investigation, the information
      shall be sealed and permission to view the files provided on a need
to know basis. Initial permission to view (not edit) will be provided
to the Deputy Chief of IAD, Undersheriff, Chief Deputy and
Sheriff.
I. When a completed personnel complaint investigation is forwarded for review, each ascending level of the chain of command shall endorse the investigation indicating either approval or disapproval for the conclusions and recommendations of the previous review level. Any level of the chain of command disapproving the recommendations or recommending some other form of disciplinary action instead of the previous review level shall submit a report to the Undersheriff or her/his assistant, detailing the reasons why. All findings shall be entered into the Sheriff’s Office electronic case management system.

J. Upon completion of the review, the personnel complaint, along with related reports, shall be forwarded to the Undersheriff.

K. The Undersheriff upon receiving a completed personnel complaint shall review and endorse the packet, indicating approval or disapproval for the conclusions and recommendations of the subordinate chain. It shall be noted that although the Undersheriff shall consult with the chain of command and/or IAD, her/his disciplinary recommendations supersede all other recommendation, except for the Sheriff’s and Chief Deputy’s. Upon completion of this review, the completed personnel complaint investigation and all related documents shall be forwarded back to the Internal Affairs Division.

L. Under no circumstances shall any level of review, which is below that of the Undersheriff change or require a change in conclusions and/or recommendations of another. When a review level does not approve conclusions and/or recommendations of another, the disapproving level shall submit a separate electronic case management system entry to the Undersheriff, indicating their own conclusions and recommendations and the reasons substantiating this belief.

M. If any level of review determines that additional investigation is required and the recommendation is approved by the Undersheriff, the further investigation shall normally be conducted by the supervisor conducting the original investigation.

N. At the end of the investigation and subsequent review by the employee's chain of command at the time the incident occurred, that chain-of-command shall discuss the complaint and all facts revealed by the investigation with all employees against whom allegations of misconduct have been made.

1. When the disposition of the matter results in a recommendation for a suspension without pay, the involved employee’s division Deputy Chief/manager shall personally conduct the discussion.

2. In the case of any other finding, the discussions may be conducted by the employee’s captain, lieutenant, or immediate supervisor at the time the incident occurred.
3. If the Deputy Chief of the involved employee, Sheriff or Chief Deputy changes the recommendation to a higher level of discipline that has been discussed with the employee, the involved employee shall be notified by the division Deputy Chief within three (3) business days of that final recommendation.

4. Recommendation for Suspension letters shall be served by the Sheriff, Chief Deputy, the Deputy Chief, Chief Inspector, Inspector, or Captain of the involved employee at the time the incident occurred or personnel in the Internal Affairs Division may serve such correspondence at the conclusion of an investigation. Any personnel serving such discipline shall ensure that the deputy fully understands the basis for the proposed suspension as well as the deputy’s Loudermill Hearing rights. A sign back shall be completed and forwarded to the Internal Affairs Division to be placed in the file.

NOTE: What is relinquishment of rights?

These rights include oral or written notice of the charges against them, an explanation of the employer's evidence, and an opportunity to be heard in response to the proposed action. Loudermill Rights are applicable in instances when the employee may have a loss of pay, such as suspension, termination, or demotion.

5. Finalized disciplinary recommendation shall not be shared with the complainant, but the complainant will receive notification from the Deputy Chief-Internal Affairs via USPS-Delivery Confirmation letter that describes the disposition of the complaint as per section VIII-D, 1-4.

6. Once disciplinary recommendations via a statement of charges, have been submitted to the employee, the Deputy Chief in the direct chain of command of the employee shall also submit a copy of the statement of the charges to the Human Resources Director.

7. The Human Resources Director shall the schedule and impanel a hearing board. The panel shall consist of two members above the rank of the employee (outside of Chain of Command) in question and a peer of the employee. The Undersheriff shall bring the charges of misconduct against the employee and shall bring evidence and witnesses to support the statement of charges.

8. The accused employee shall have the right to union representation and to present evidence and bring witnesses to support her/his claims.

9. After all evidence and witnesses have been presented, the panel shall render a decision as to the culpability of the employee and the disciplinary actions, if any to be taken against the employee.
10. A Finding Form shall be submitted to the Sheriff, detailing the hearing
panel’s findings and reasons for coming to those findings. The Sheriff shall
verify the panel’s findings or arrive at findings of her/his own. The
Sheriff’s verification or findings are final.

1. In the case of any other finding, the discussions may be conducted by the
employee’s captain, lieutenant, or immediate supervisor at the time the incident
occurred.

2. If the Deputy Chief of the involved employee, Sheriff or Chief Deputy changes
the recommendation to a higher level of discipline that has been discussed with
the employee, the involved employee shall be notified by the division Deputy
Chief within three (3) business days of that final recommendation.

3. Suspension letters shall be served by the Sheriff, Chief Deputy, the Deputy Chief,
Chief Inspector, Inspector, or Captain of the involved employee at the time the
incident occurred or personnel in the Internal Affairs Division. Any personnel
serving such discipline shall ensure that the deputy fully understands the basis for
the suspension as well as the deputy’s Loudermill Hearing rights. A sign back
shall be completed and forwarded to the Internal Affairs Division to be placed in
the file.

4. Finalized disciplinary information will not be shared with the complainant, but the
complainant will receive notification from the Deputy Chief-Internal Affairs via
USPS-Delivery Confirmation letter that describes the disposition of the complaint
as per section VIII-D, 1-4.

K. Minor incidents which will not reflect discredit upon the Office of the Sheriff, but
which indicate a need for some form of corrective action and/or training (any offense
that could incur a maximum of one day or below with aggravating circumstances
factored), may be dealt with by the involved employee’s immediate supervisor with
the review and concurrence of the involved employee’s Captain.

L. The Personnel Complaint form shall not be completed when complaints are solely
against department policies or procedures. If a complaint is determined to be
concerning department policies or procedures and no misconduct is indicated, and the
incident cannot be explained to the complaining person’s satisfaction, that person
shall be referred to the organizational entity having administrative control over the
subject matter.

M. Complaints from Intoxicated Persons or a Third-Party Source.

1. When a personnel complaint is received from an intoxicated person, a Personnel
Complaint form shall be prepared and processed, without the complaining
person’s signature. The complaining person shall be re-interviewed at the earliest
opportunity after having regained sobriety by the supervisor assigned the
investigation. During the re-interview, the complaining person shall be asked to
sign the Personnel Complaint form. Refusal to sign the form will not invalidate the complaint process.

2. When a personnel complaint is received from a third-party source, a complaint form shall be prepared and processed. The third-party source shall be asked to sign the Personnel Complaint form as the reporting party.

3. In either event, unless the personnel complaint is validated by subsequent interview of the intoxicated person or an actual party to the incident, the final disposition of such complaint shall not be listed on a deputy’s Internal Affairs Division record. All reports related to such complaints shall be filed as miscellaneous memorandums by the Internal Affairs Division.

N. The personnel complaint form shall be completed on personnel complaints received from anonymous sources; however, when information is received by a supervisor which originated from an anonymous source, the supervisor shall submit the anonymous complaint via memorandum, detailing the information received, and forward it to the Internal Affairs Division.

1. If the information received is of a nature that would jeopardize the integrity of an investigation by being reduced to writing, it shall be communicated via telephone to the Deputy Chief of Internal Affairs or Undersheriff via telephone.

2. If the information received describes misconduct of a nature which, if true, would normally result in a form of disciplinary action in excess of 1-day suspension or more, a preliminary investigation will be conducted.

3. When warranted, the allegation of misconduct shall be reported on a Personnel Complaint form. If the identity of the anonymous reporting party cannot be determined or if identified, refuses to sign the Personnel Complaint form, the signature of the investigating supervisor in the “complainant” block will be considered a valid substitute for the signature of a reporting party.

LXXVI. DISCIPLINARY PROCEDURES: SENSITIVE INVESTIGATION

O. When a personnel complaint or incident is of a nature that the integrity of the investigation may be compromised or jeopardized by reducing the incident to writing, the reporting supervisor shall immediately report the incident to their commander, who shall report said incident to the Deputy Chief Internal Affairs Division.

P. If the reporting supervisor has reason to believe the integrity of the investigation may be compromised by passage through normal channels, the supervisor shall personally report the incident directly to the Deputy Chief Internal Affairs Division.
Q. When immediate action is required or the seriousness of the incident is such that it may subject the Office to severe criticism or liability, the reporting supervisor shall provide immediate notification to the involved employee’s division commander and to the Deputy Chief Internal Affairs Division.

1. In incidents of this magnitude, division Deputy Chiefs may temporarily relieve the involved employee from duty, with pay, and shall, when applicable, take custody of a deputy’s badge, identification card, and service weapon.

LXXVII. DISCIPLINARY PROCEDURES: SUPERVISOR RESPONSIBILITY

A. Supervisors/Captains who become aware of alleged misconduct shall:

1. Ensure that a Personnel Complaint form is prepared without unnecessary delay and signed by the interviewing supervisor and the reporting party.

2. Ensure that an appropriate preliminary investigation has been completed.

3. Ensure that all complaint forms, copies, and related reports are forwarded to the appropriate personnel as described in this directive and that all notifications required are completed.

4. The investigator or supervisor performing the investigation shall provide the employee with the written allegations in the complaint no less than 48 hours before the initial interview or requesting any memorandum or other correspondence related to the incident from the employee.

NOTE: The 48-hour notice does not apply to on-scene investigations that occur immediately after an incident.

B. Deputy Chiefs have the primary responsibility for investigating personnel complaints made against employees of their commands. A Deputy Chief who becomes cognizant of any allegation of misconduct shall monitor all resulting activities and shall ensure that personnel under their command have fulfilled their responsibilities provided in this order. A deputy chief may request that the Internal Affairs Division conduct an investigation on any allegation of misconduct or personnel complaint.

LXXVIII. DISCIPLINARY PROCEDURES: INTERNAL AFFAIRS DIVISION RESPONSIBILITIES

A. The Deputy Chief of the Internal Affairs Division shall act in a staff advisory capacity when necessary. The deputy chief may assume responsibility for the investigation of
any personnel complaint when, in the opinion of the deputy chief, it is advisable to do so.

B. The Internal Affairs Division shall assume responsibility for a personnel complaint when:

1. It has been alleged an employee has committed any felony or Class A or B misdemeanor.

2. The allegation of misconduct is against employees of more than one division.

3. The investigation involves an allegation of:

   a. Excessive force,
   b. Sexual harassment,
   c. Hostile work environment,
   d. Disparate treatment due to gender, race, ethnicity, age, or sexual orientation,
   e. Retaliation for reporting the misconduct of another,
   f. Inappropriate conduct or comment of a sexual nature, or
   g. Inappropriate comment regarding gender, race, ethnicity, age, or sexual orientation.

C. The Deputy Chief-Internal Affairs Division has the authority to obtain the advice and assistance of any departmental entity.

D. In the event an Assigned Investigator is unable to contact a complainant or witness for interview (or follow-up investigative statements) the Deputy Chief of Internal Affairs will ensure the Assigned Investigator exercises due diligence to contact the complainant or witness. Due diligence shall include at least two visits to the last known address of a complainant/witness and mailing a certified letter with delivery confirmation via USPS. Every contact attempt will be separately logged into the IAD Pro file.

LXXIX. **ARRESTED SHERIFF’S OFFICE EMPLOYEE**

A. If an employee of the department is detained or arrested for any criminal offense within the City of Philadelphia, the deputy detaining or arresting the employee shall immediately notify a supervisor of the division/jurisdiction in which the employee is detained or arrested.

B. A supervisor who has been notified that an employee of the department has been arrested or detained shall immediately proceed to the scene and shall ensure that the Deputy Chief-Uniform Services is immediately notified.
C. The Deputy Chief-Uniform Services shall ensure immediate notification is made to:

1. The Internal Affairs Division Deputy Chief.

2. The Deputy Chief of the employee’s division of assignment.

3. The employee’s Captain or director.

4. The Public Information Deputy.

D. When a need is indicated to present to the jail an employee who has been arrested, the Deputy Chief-Internal Affairs shall contact the involved employee’s bureau deputy chief or assistant department head for booking approval. If the involved employee’s deputy chief or assistant department head is unavailable, the duty deputy chief shall be contacted for booking approval.

E. The deputy chief or Undersheriff shall determine if the employee is to be presented to the appropriate jurisdiction jail for booking.

   1. If no deputy chief is available, the Deputy Chief of Internal Affairs Division shall make the determination as to whether booking shall take place.

F. The Internal Affairs Division or the appropriate specialized investigative unit shall investigate whenever an employee is arrested for or believed to be a principal suspect in a felony or M1 or M2 offense. When applicable, they shall be responsible for submitting the criminal case to the District Attorney for consideration of criminal prosecution. The Deputy Chief-Internal Affairs Division has the discretion to assume responsibility for investigations related to class M1 violations.

G. When any employee of the department is detained or becomes aware that they are believed to be the principal suspect in a criminal offense, other than minor traffic violations committed outside the City of Philadelphia, the employee shall as soon as possible notify a on call, or on-duty supervisor.

H. When any employee of the department becomes aware that another employee has been detained or is believed to be a principal actor in a criminal offense, other than minor traffic violations committed outside the city, the employee shall immediately notify an on call or on duty supervisor.

I. Any supervisor who is notified regarding the detention or arrest of an employee by another law enforcement agency, other than minor traffic violations, shall ensure that immediate notification is made to the Internal Affairs Division and to the applicable Divisional Deputy Chief of the involved employee.
J. The on-call or working Internal Affairs Division investigator shall respond to the scene or to the indicated outside agency (within a 3-hour radius) when the incident involves an alleged felony, M1, or M2 violations.

1. A supervisor from the involved employee’s division of assignment shall respond on alleged class C misdemeanor violations if the violation is of a magnitude to require immediate investigation and is within a 1-hr radius.

   a. Regardless of whether a supervisor responds to the scene, a Personnel Complaint form shall still be prepared and processed.

2. The responding supervisor shall conduct a preliminary investigation and a Personnel Complaint form shall be prepared, processed, and added to IA PRO/Blue Team.

3. The responding supervisor shall advise concerned members of the outside agency that the preliminary investigation is for internal administrative purposes only and that any evidence obtained by the responding supervisor solely as a result of interviewing the involved employee shall not be disclosed to the agency conducting the criminal investigation. Responding supervisors shall exercise extreme care not to interfere with the investigation of the outside agency.

LXXX. **DISPOSITION OF ADMINISTRATIVE INVESTIGATIONS**

A. Administrative investigations which may result in disciplinary action, whether conducted by the Internal Affairs Division or the involved employee’s division of assignment, shall be completed within thirty-one (31) calendar days from the date the complaint is received or initiated.

Note: Due to the complicated nature of some investigations, the investigation deadline may be waived by the division Deputy Chief or Undersheriff but will not exceed 179 days.

B. Unless approved by the Sheriff or designee, a recommendation of potential charges (if warranted) is the responsibility of the division investigating the incident.

C. If the incident is minor, as described in this directive, the complete administrative investigation prior to the issuance of any discipline will be the responsibility of the chain of command of the deputy at the time of the incident or misconduct. **If an employee is transferred/moved prior to the completion of the investigation, the chain-of-command responsible for that employee at the time the incident occurred will continue the investigation, review, and notifications. Reassignment of the deputy does not reassign responsibility of any part of the investigative, notification or discipline process.**
D. If the incident or offense is investigated by the Internal Affairs Division, the complete administrative investigation AND recommendation for subsequent action will be made by the Internal Affairs Investigator.

E. The review by the chain of command or the IAD Investigator, including letters of transmittal or files via IAD Pro or Blueteam, shall be completed within fifteen (15) calendar days of the date the investigation is completed or the date the investigative report is received from the Internal Affairs Division.

F. A completed investigation shall be submitted to the involved employee’s division Deputy Chief by the supervisor of same through the chain of command via Blue Team and shall include a summary of facts prepared by the employee’s Captain with an appropriate conclusion, classifying each specific act of misconduct into one of the following categories:

1. **Unfounded**: The investigation reveals sufficient evidence to believe the complained of act did not occur.

2. **Exonerated**: The investigation reveals the complained of act occurred but was legal, proper, and justified.

3. **Not Sustained**: The investigation discloses insufficient evidence to believe the complained of act either did or did not occur.

4. **Sustained**: The investigation discloses evidence that is sufficient to conclude the complained of act occurred.

G. When an investigation subsequently discloses additional allegations of misconduct which were not described in the original personnel complaint and the classification of the original complaint is other than sustained, a new complaint form shall be prepared, and a supplemental investigative report completed. When any allegation of misconduct in the original personnel complaint is sustained, the new allegations may be recorded as separate supplemental charges in the investigative report for the original complaint.

H. If any allegation of misconduct is sustained, the employee’s first-line supervisor at the time the incident occurred shall:

1. Prepare the summary report.

2. Discuss the summary report with the applicable chain of command, i.e., sergeant will discuss the complaint with the lieutenant and captain and enter a collective recommendation for disciplinary action.
a. The recommendation should be within disciplinary matrix guidelines and should factor the severity of the offense and any aggravating factors if they exist.
b. The deputy's personnel record should also be assigned weight.
c. Discuss the findings and recommendation for disciplinary action with the involved employee in person, documenting the meeting in the summary report.

3. Forward the completed investigation and summary report for review by the remaining layers of the employee's chain of command via Blue Team.

a. If the finding is a result of a criminal investigation, the information shall be sealed and permission to view the files provided on a need to know basis. Initial permission to view (not edit) will be provided to the Deputy Chief, IAD, Undersheriff, Chief Deputy and Sheriff.

I. When a completed personnel complaint investigation is forwarded for review, each ascending level of the chain of command shall endorse the investigation indicating either approval or disapproval for the conclusions and recommendations of the previous review level. Any level of the chain of command disapproving the recommendations or recommending some other form of disciplinary action of the previous review level shall personally discuss their recommendations with the involved employee, documenting the meeting in the report within Blue Team.

J. Upon completion of the review, the personnel complaint, along with related reports, shall be forwarded to the involved employee's deputy chief.

K. A deputy chief receiving a completed personnel complaint shall review and endorse the packet, indicating approval or disapproval for the conclusions and recommendations of the subordinate chain. Upon completion of this review, the completed personnel complaint investigation and all related documents shall be forwarded back to the Internal Affairs Division.

L. Under no circumstances shall any level of review change or require a change in conclusions and/or recommendations of another. When a review level does not approve conclusions and/or recommendations of another, the disapproving level shall submit a separate Blue Team entry indicating their own conclusions and recommendations and the reasons substantiating this belief.

M. If any level of review determines that additional investigation is required, the further investigation shall normally be conducted by the supervisor conducting the original investigation.

N. At the end of the investigation and subsequent review by the employee's chain of command at the time the incident occurred, that chain-of-command shall discuss the
complaint and all facts revealed by the investigation with all employees against whom allegations of misconduct have been made.

5. When the disposition of the matter results in a recommendation for a suspension without pay, the involved employee’s division Deputy Chief/manager shall personally conduct the discussion.

6. In the case of any other finding, the discussions may be conducted by the employee’s captain, lieutenant, or immediate supervisor at the time the incident occurred.

7. If the Deputy Chief of the involved employee, Sheriff or Chief Deputy changes the recommendation to a higher level of discipline that has been discussed with the employee, the involved employee shall be notified by the division Deputy Chief within three (3) business days of that final recommendation.

8. Suspension letters shall be served by the Sheriff, Chief Deputy, the Deputy Chief, Chief Inspector, Inspector, or Captain of the involved employee at the time the incident occurred or personnel in the Internal Affairs Division. Any personnel serving such discipline shall ensure that the deputy fully understands the basis for the suspension as well as the deputy’s Loudermill Hearing rights. A sign back shall be completed and forwarded to the Internal Affairs Division to be placed in the file.

9. Finalized disciplinary information will not be shared with the complainant, but the complainant will receive notification from the Deputy Chief-Internal Affairs via USPS-Delivery Confirmation letter that describes the disposition of the complaint as per section VIII-D, 1-4.
DIRECTIVE: #56

SUBJECT: CODE OF CONDUCT

ISSUE DATE: 04-10-2020

REVISED DATE: 02-16-2020

LXXXI. PURPOSE:

A. This directive establishes a Code of Conduct for employees of the Office of the Philadelphia Sheriff officially adopted and set forth in this manual and enacted by the Sheriff and takes precedence over other regulatory Directives. The Code of Conduct provides rules and regulations for the regulation of employee conduct and shall serve as this Office’s directives, rules and regulations, general orders and/or policies.

B. Pursuant to section Philadelphia City Charter, the Sheriff shall have immediate control and direction of the Philadelphia Sheriff’s Office, and exercises the right within collective bargaining agreement (contract” with the FOP Lodge 5) shall promulgate all orders, rules and regulations, make assignments, prescribe the uniforms and badges for members of the Sheriff’s Office, and direct the manner in which the members of said force shall be armed.

C. The Sheriff, or designee, shall have the power to take disciplinary action or suspend indefinitely a deputy or employee for violation of this Code of Conduct, Directives, or the regulations contained in the City of Philadelphia Employee Rules and Regulations.

D. The provisions of the contents within this directive shall be observed by all members of the Office of the Sheriff in order to maintain the confidence, respect, and support of the public. Deputies of the Philadelphia Sheriff’s Office shall acquire a working knowledge of the Directives, special orders, city ordinances, PA Rules of Criminal Procedure, the PA Crimes Code, PA Rules of Civil Procedure, federal statutes, and current court cases.

E. All Deputies and employees shall comply with the Directives, special orders, Directives, procedures of the Sheriff’s Office, orders and instructions of supervising
Deputies, federal law and regulations, state law and regulations, and city ordinances and regulations.

F. Code of Ethics:

1. As an employee of the Philadelphia Sheriff's Office, my actions will be guided by the following principles: Justice, Excellence, Humility and Harm Reduction. Our Office’s goals focus on ensuring that all parties in civil and criminal litigation are treated fairly and are able safely exercise the rights and duties relating to the Pennsylvania Judicial System without encumbrance. We also hold that throughout the legal process, respect for the dignity and humanity of each participant is displayed and observed by all members of our Office. We also strive to pursue these goals via time tested tactics, available research, innovation, training and partnering with the community. As a member of law enforcement entrusted and empowered by my community to protect all of our community (Sheriff’s Office employees and community members alike), I will strive to display the values of:

   a. **Justice** - I will treat people fairly and act in good faith. I will work toward racial and social justice for all.

   b. **Excellence** - I will not be satisfied with the status quo. I will review all systems and processes with an eye towards improvement, efficiency, and professionalism. When I attend training or review new policies, I will strive to master the material because I recognize that training leads to competency.

   c. **Humility** - I will learn from both positive and negative experiences and share what I learn with others. I will listen to what other people are saying, ask questions and consider their concerns.

   d. **Harm Reduction** - I will commit to exploring new ways to improve public safety, and to protect property owner rights, while reducing harm to vulnerable communities and individuals. I will think outside the box and look for long-term and sustainable solutions while partnering with others.

   e. **Service** - The common thread tying these four principles together is service. Service is my mantra, and I will keep service to our community as my first priority. I will provide that service with pride and dedication.

2. Crime prevention and crime fighting are also integral parts of our mission; and are expectations in all law-enforcement functions. Effective crime fighting requires community problem solving. Community problem solving requires both the Sheriff's Office personnel and community members to take responsibility for involving each other in our efforts. Community trust is built one transaction at a time. Sheriff’s Office employees (sworn and civilian) and community members who work together strengthen that bond and can build safer, stronger, and more compassionate...
communities. Harm reduction represents an acknowledgement that there are competing interests, demands, and strains on our social structures that create particularly challenging opportunities for law enforcement, especially as they relate to housing and predatory lending practices. These opportunities include finding long-term sustainable ways to reduce the harm caused by various fiscal challenges within our community while leveraging these opportunities to fortify bonds of trust between the Sheriff’s Office and the communities we serve.

3. As an Office of the Sheriff employee, I am responsible for supporting the mission and principles of the Philadelphia Sheriff.

G. Ignorance of any provision contained in the Directives, special orders, the Code of Ethics, or other training or policies shall neither be an excuse nor serve as a defense for a violation of these materials.

1. In the event of improper action or breach of discipline, it shall be presumed the deputy was familiar with the law, directive, order, or policy in question.

H. Deputies and employees, whether on-duty or off-duty, shall follow the Directives, special orders, and policies of the Sheriff’s Office regarding good conduct and behavior and shall not commit any act in an official or private capacity that would be an applicable violation of any Directive, special order, policy or procedure.

I. No member of the Office of the Sheriff shall wear their uniform or carry a pistol while under suspension for any cause.

J. No deputy shall procure appointment in the Office by means of intentional misrepresentation or omission of any fact concerning personal history, qualifications for employment, or physical condition.

K. All employees or candidates for employment must submit to a physical and/or psychological examination when directed by the Sheriff.

L. Non-Commissioned Deputies within the probationary period of employment may be terminated by the Sheriff without cause when they fail to meet the minimum standards of the Pennsylvania Commission on Crime and Delinquency, employee performance or when they violate the Directives, Civil Service Rules and Regulations, City of Philadelphia Personnel Rules and Regulations, City Charter provisions, ordinances, city codes, federal law or the laws of any state.

M. All employees shall diligently attempt to resolve any matters of fines or financial responsibilities in a timely manner. Employees shall not allow any personal fine or
legal action progress to a warrant against the employee. At any time, the employee
learns a warrant has been issued against them, the employee will notify their
supervisor immediately and contact the issuing Office of the Sheriff immediately to
resolve the situation.

LXXXII. PROFESSIONAL CONDUCT


B. Abuse of Alcohol / Controlled Substances / Prescription Drugs – Defined Charges in
Duty Manual-Article II, p. 31-32, Amended to include the following:

1. Consuming THC, Marijuana, Hemp, or CBD oil beverages, or while on duty.
   Dismissal

2. Use of unprescribed drugs, narcotics, or medical marijuana. Use of substances
   that alter alertness or inhibit reaction time or mood shall not be permitted while
   on-duty-Dismissal

3. Use of MDMA, LSD, Khat, K2, Hyro, Peyote, Mushrooms or Hallucinogenic
   Drugs. - Dismissal


D. Insubordination– Defined Charges in Duty Manual-Article IV, p. 34-35

   36-41, Amended to include the following instances (ranging from 10 days off to
   Dismissal):

1. Neglect of duty is defined as the abandonment, either through omission or
   commission, intentional or otherwise, of any duty which has been designated to
   an employee of the Sheriff’s Office, whether through the Directives, special
   orders, orally, or through written directive from a superior. The assignment of the
   duty may be either explicit or implicit.

2. Neglect of duty on the part of any employee is cause for disciplinary action. The
   offender shall be disciplined according to the severity of the violation, the
   commensurate responsibility or accountability of their rank or position, the results
   brought about by the action or inaction, and the effect it has upon the discipline,
   good order, and best interest of the Office of the Sheriff.

3. Neglect of duty also expressly includes, but is not limited to, the following:
a. Failure of a supervisor to immediately act when a violation of rules or regulations comes to their attention, regardless of the supervisor’s or violator’s assignment or rank within the Sheriff’s Office.

b. Failure to observe and give effect to the federal, state, and local statutes and the directives of the Sheriff’s Office.

c. Failure to deliver to an official Sheriff’s Office custodian any property found, confiscated by, or relinquished to employees of the Office of the Sheriff without undue delay and at least prior to the end of their shift.

d. Failure to place any item confiscated in its officially designated place for preservation and storage.

e. Failure to give name and identification number to any person upon request, unless otherwise officially excepted.

f. Using unnecessary and/or excessive force, toward any person.

g. Being disrespectful to any person.

h. Use of indecent, profane, or harsh language in the performance of official duties.

i. Accepting, agreeing to accept, or soliciting a bribe. A bribe is defined as a gift, emolument, money, thing of value, testimonial, appointment or personal advantage, or the promise or solicitation of same for the purpose of obtaining special privileges or personal gain by the donor or other person.


G. Failure to Supervise (5 days to Dismissal)/Failure to command (10 days to Dismissal)—Defined Charges in Duty Manual-Article VII, p. 43, Amended to include the following:

1. New definitions

   a. **Command** - Refers to authority and responsibility to direct the operations of a bureau, division, section, unit, or detail. The actions for this position will be held accountable to a higher standard due to compensation, leadership, training, knowledge, education, and ability to motivate employees.

   b. **Commander** shall in general refer to persons holding the rank of deputy chief, captain, lieutenant, or equivalent civilian classifications.

2. Responsibilities of command shall include, but not be limited to:

   a. Direction of the operations of an organizational entity.

   b. Oversight of an organizational entity to ensure compliance with applicable laws, rules, regulations, and orders emanating from higher ranks.

   c. Developing and recommending policies and procedures affecting functions of the entity being commanded.

   d. Planning of operations, both short-term and long-range.

   e. Administration of discipline.
f. Ensuring that descending levels of personnel are kept informed of necessary items, including policies, procedures, and operational changes.
g. Providing information to ascending levels of rank as to the conformance to policies and procedures.
h. Administration and management of an organizational entity to include establishing and monitoring the budget, selection of personnel, ensuring proper supervision is utilized, provision of necessary supplies and equipment, obtaining adequate training for assigned personnel, monitoring the productivity of personnel.
i. Implementation of strategies and policies set forth by the Sheriff as defined by job description (all ranks above lieutenant).

3. **Failure to supervise** as defined by job description (all supervisory ranks above Deputy Sheriff Officer). Failure to protect the property belonging to a person in custody or property which has come into possession of the deputy by reason of their office. No deputy shall ridicule, mock, deride, taunt, or belittle any person. Neither shall the deputy knowingly embarrass, humiliate, or shame any person nor do anything that might incite such person to violence.

4. **Supervision** - To provide oversight, direction, and control of employees or an organizational entity below a section. The actions for this position will be held accountable to a higher standard due to compensation, leadership, training, knowledge, education, and ability to motivate employees.

5. **Supervisor** in general shall refer to anyone with the responsibility of supervising a subordinate employee and as a class shall denote a sergeant or equivalent civilian classification.

6. **Responsibilities of supervision** shall include, but not be limited to:

   a. Monitoring the performance of subordinates to ensure appropriate levels of productivity and to ensure that employees comply with all laws, rules, regulations, and orders.
   b. Initiating disciplinary or remedial action towards employees who violate any law, rule, regulation, order, or who fail to maintain appropriate levels of productivity.
   c. To either deliver, or cause to be delivered, appropriate training for subordinate employees.
   d. To assume accountability for the actions or non-actions of all subordinate employees.
   e. To direct and control the operations of a unit, detail, or district, including issuance of orders or instructions, review, and correction of work products, setting work priorities, and appropriating necessary supplies and equipment.
   f. Administration and management of an organizational entity to include establishing and monitoring the budget, selection of personnel, ensuring proper supervision is utilized, provision of necessary supplies and equipment,
obtaining adequate training for assigned personnel, monitoring the productivity of personnel.
g. Implementation of strategies and policies set forth by the Sheriff as defined by job description (all ranks above lieutenant).

4. Proper judgment, demeanor, courtesy, and discretion are mandatory, both within the Sheriff's Office, and when interfacing with the public. The use of words or gestures which are derogatory or inflammatory in nature to or about any person or group of persons, because of their race, color, gender, age, national origin, religion, disability, economic status, sexual orientation, gender expression, gender identity, transgender status, membership in a cultural group, or other individual characteristics or distinctions or taking any discriminatory actions is strictly prohibited.

5. The following appropriate terminology or combination thereof shall be the only terms used by Sheriff's Office employees to describe certain persons, unless required otherwise by the necessity to state quotes in official reports using terms, words, phrases, or expressions actually spoken.

a. Female Person: Female, woman, subject, suspect, juvenile, offender, person.

b. Male Person: Male, man, subject, suspect, juvenile, offender, person.

c. Non-binary person: The term “non-binary” can mean different things to different people. At its core, it’s used to describe someone whose gender identity isn’t exclusively male or female.

1) If someone tells you they’re non-binary, it’s always important to ask what being non-binary means to them. Some people who are non-binary experience their gender as both male and female, and others experience their gender as neither male nor female.

2) Non-binary can also be used as an umbrella term, encompassing many gender identities that don’t fit into the male-female binary.

d. Gender-Neutral Person: use pronouns that do not associate with a gender, such as they or it. In English, the term gender-neutral pronouns usually refers to third-person pronouns (generally alternatives to he and she), since there are no gendered first- or second-person pronouns (I, you, they, them, their, are ungendered).

e. Black Person: Black, African American.

f. White Person: White, Caucasian.

h. Undocumented Migrant: Non-registered or undocumented migrant/person.

i. Foreign National: Mexican-national, French-national, Canadian-national, e.g., (country of origin) national.

j. Asian Person: Asian, Pacific American, Asian/Pacific Islander.

k. Physically disabled: Person with physical disability, physically challenged, physically disabled.

l. Mentally disabled: Person with mental disability, mentally challenged, mentally disabled, mentally disturbed, or person in crisis.

6. Within Philadelphia City/County: Deputies shall at all times take appropriate action to:

a. Protect life and property.

b. Preserve the peace.

c. Prevent crime.


e. Promptly respond to all calls for service and provide quality service.

f. Accept and enforce civil actions, injunctions, writs, etc.

g. Enforce and abide by all federal, state, and local laws and ordinances within the Sheriff’s Office jurisdiction.

h. When off-duty and/or in a personal vehicle, even if in uniform, enforcement of summary violations or low-level misdemeanors shall be allowed only when there is an immediate danger of a breach of the peace or danger to persons or property.

Deputies shall, at all times, respond to the lawful orders of supervisors and other proper authorities as well as requests for law enforcement assistance from citizens. The administrative delegation of the enforcement of certain civil laws and ordinances to particular units of the Sheriff’s Office does not relieve Deputies of other units from the responsibility of taking prompt, effective law enforcement action within the scope of those laws and ordinances when the occasion so requires. Deputies assigned to special duty are not
relieved from taking enforcement action outside the scope of their specialized assignment when necessary. All members shall perform their duties as required or directed by law, Sheriff’s Office rules, policies, or by orders of a supervisors.

a. If an employee receives an order that conflicts with one previously given them by a supervisor, the employee receiving the order shall respectfully point this out to the supervisor who gave the second order. If the supervisor giving the second order does not change the order in a way that eliminates the conflict, the second order shall stand and shall be the responsibility of the second supervisor.

b. If the second supervisor so directs, the second order shall be obeyed first. Orders shall be countermanded only when necessary for the good of the Sheriff’s Office.

7. Deputies shall not address public gatherings, appear on radio or television, prepare any articles for publication, act as correspondents to a newspaper or periodical, release or divulge internal Sheriff’s Office information, or any other matters of the Sheriff’s Office while holding themselves out as representing the Sheriff’s Office in such matters without proper authority. Deputies may lecture on law enforcement or other related subjects only with the prior approval of the Sheriff.

a. Deputies, authorized by assignment, rank, or specialized training, will not be restricted from addressing community law enforcement functions or granting interviews at police-related incidents if no conflict exists with another Directive, i.e., Critical Deputy Incident, Release of Information, etc.

b. Any employee who is contacted by the news media for an interview or for information shall immediately notify the Public Information Office (PIO) by telephone or e-mail with the name of the person requesting the information or interview, the substance of the interview, and if applicable, copies of any materials provided. Contacting the PIO will not be necessary if the request for information or an interview was directed to the employee by the PIO.

8. Deputies are required to take appropriate law enforcement action to aid a fellow law enforcement officers exposed to danger or in a situation where danger might be impending.

9. Employees are prohibited from engaging in the following activities while on duty:

a. Sleeping.
b. Drinking intoxicating beverages, except in performance of their duties, and then only by the specific direction of a supervising deputy, and never in uniform.

c. Reporting for duty when it is apparent, they have consumed intoxicants, or being intoxicated while on duty.

d. Gambling, except in performance of law enforcement duties, and then only by the specific direction of a supervisor, and never in uniform.

e. Use of narcotics (as specified in IIA-3k).

10. Employees shall not bring any intoxicating liquor into any Sheriff’s Office facility or city vehicle, except in the line of duty or as evidence.

11. While on or off duty, employees shall not use any illegal drug, or any controlled drug not prescribed or not used as prescribed by a physician. A deputy who is not fit for duty due to injury, illness or certain medications should follow the call-off procedures and not report for duty unless on approved light duty.

a. Employees should be aware that restrictions on driving, whether caused by physical conditions or medications, do not relieve employees of the responsibility to report to work, absent further restrictions or issues that would take them off work. Therefore, employees with driving restrictions who choose not to utilize public transportation or other methods for traveling to and from work must obtain permission from their supervisors to take off work and must use their own paid leave for that purpose. No employee with a valid restriction against driving will be required to drive while at work for work purposes.

12. The use of smokeless tobacco products shall be prohibited by Deputies on duty and by Deputies off-duty who are in uniform. No deputy shall smoke or chew gum while making personal contact with citizens in the performance of duty.

a. In accordance with the City of Philadelphia Regulations, “Smoking in the Workplace,” employees are prohibited from smoking in any city vehicle or facility.

13. No unprofessional poster, picture, or slogan shall be displayed in any the Sheriff’s Office facility or vehicle. This shall include any display of a sexually explicit/graphic nature and any material which may be offensive to the public or other employees. Supervisors will conduct quarterly audits of their workplace to assure compliance.

14. Deputies deployed to a Uniform Services Division assignment such as posts in CJC, City Hall, Traffic Court, or 1501 Arch, shall devote their full attention to
duties within that assignment. Deputies may leave their assignment when required by reason of being dispatched via radio and call-sign to another area or to perform activities directly related to their assigned duties, i.e., calls, reassignments, response to assist calls from other Deputies, crime outside of their courtroom or courthouse building, etc.

a. Deputies shall obtain supervisory approval to leave their assignment for any other reason than directly related to duty.

b. Deputies shall inform the desk supervisor via radio of their intended destination and purpose when leaving geographic assignment for any reason other than by dispatch authority.

c. Deputies shall use the most direct route to and from any activities which require the deputy to leave an assignment.

d. Unless otherwise directed, supervisors shall remain in the field to monitor and supervise their subordinates.

e. Personnel such as warrant unit, civil enforcement, or transportation unit deputies whose duties normally require travel across geographic areas will not be required to obtain dispatch approval before crossing geographic boundaries.

15. While on-duty or off-duty and carrying a firearm, all Deputies shall have their badge, Sheriff’s Office identification card, and current and unexpired commission card in their possession.

a. A captain or above may grant temporary permission to forego this requirement to on-duty deputies in an undercover or other special capacity.

16. While on-duty, all Deputies are required to have in their possession a valid Commonwealth of Pennsylvania driver’s license.

17. In each contact with the public, deputies shall be aware their actions, appearance, and statements are those of the Sheriff’s Office. For that reason, all interactions with persons encountered through official duties shall be conducted with the highest professional and ethical standards.

a. Deputies shall refrain from initiating or responding to an invitation for a social relationship with a complainant, victim, witness, suspect, arrested person, or contact both during the initial encounter and while they have court cases pending.
b. Employees will not knowingly associate with convicted felons if doing so will bring about justified unfavorable criticism to the Sheriff's Office. This policy is not meant to discourage efforts to rehabilitate persons with criminal records or to prevent deputies from all communication with family members.

18. Arrests:

a. No deputy shall arrest any person or search any premises or persons except with a warrant of arrest, a search warrant, or where such arrest or search is authorized without a warrant by law.

b. No deputy shall falsely arrest, imprison, or cause any malicious prosecution to be instituted against any person.

19. All Deputies shall protect the rights of any person held in custody. No deputy shall verbally abuse or use unnecessary force against any such person, nor allow another deputy or individual to do so.

a. Deputies are required to protect the rights of all persons and are prohibited from engaging in any form of discrimination, oppression, or favoritism.

LXXXIII. CIVIL, CRIMINAL, JUDICIAL, AND INVESTIGATIVE ACTIONS

A. The Sheriff's Office has primary jurisdiction in civil cases and the ability to act upon violations of criminal law. No deputy shall investigate, intervene, render aid or assistance to resolve civil or criminal cases or disputes except to prevent an immediate breach of the peace or to quell a disturbance in progress. This regulation is not intended to prevent Deputies from advising citizens that a civil remedy may exist.

B. Deputies shall not purchase property directly or indirectly (via sole-proprietorship, LLC, Inc, Board Member or holding interest of any kind in any entity, through a Philadelphia Sheriff’s Sale.

C. Deputies shall not engage in any of the following conduct:

1. Interfering with the service of lawful process.

2. Interfering in any way with the attendance or testimony of witnesses.

3. Attempting to have any court record, writ, warrant, injunction, action, or citation erased removed, reduced, voided, or stricken from the calendar or record except in a manner prescribed on mitigation of state or municipal court cases.

4. Recommending a dismissal, reduction of charges, or other disposition of a pending civil or criminal case except by prior written approval of the Sheriff.
5. Interfering in any way with the attendance or testimony of witnesses.

6. Taking any other action which impedes the efficiency or integrity of the administration of criminal justice.

7. Failing to inform a supervisor in writing of such interference either by their own actions or by another deputy when having knowledge of same.

8. Deputies shall not wear the Sheriff's Office uniform when testifying in criminal or civil court unless the testimony is directly related to their position as a Philadelphia Deputy Sheriff.

D. Deputies shall not suggest, recommend, advise, solicit on behalf of, or otherwise counsel the retention of any specific attorney or bail bond broker to any person as a result of Sheriff’s Office business.

E. Deputies shall not furnish bail or act as a principal or surety on any bail bond or bail bond application for personal gain of goods or services, for any person charged with a civil or criminal offense.

F. No deputy shall personally investigate any criminal case, or personally file any criminal charge, for an offense committed against them personally or any member of their family or which may involve the deputy or family member as a witness to the offense(s). Criminal offenses involving deputies, or their family members shall be reported to the division of the police department having responsibility for the investigation of such offenses. This regulation is not intended to prevent deputies from taking appropriate action if a crime is being committed in their presence.

G. Deputies and civilian employees shall be truthful, candid and make full disclosure of all relevant and material information at all times when responding to supervisors and/or co-workers, while testifying in court, while testifying under oath at a deposition, while testifying at any administrative proceeding, and while responding to an administrative or internal investigation.

1. Employees shall be truthful at all times in their dealings with co-workers, supervisors, managers, and other law enforcement personnel. Any statement or omission of pertinent or material information which misrepresents facts or misleads others will be considered a false statement.

H. Deputies and civilian employees shall answer all questions candidly, provide full disclosure, and give material and relevant statements when requested by any appropriate authority in a departmental administrative or internal investigation.

I. No deputy or civilian employee shall knowingly misrepresent any matter, make a false statement or report, commit perjury, mislead, or give false testimony before any court, grand jury, board, commission, official hearing, or departmental hearing.
J. No deputy or civilian employee shall knowingly falsify any report, document, or record nor cause to be entered any inaccurate, false, or improper information on records, documents, or reports of the department or of any court, or alter any record, document, or report.

K. Reports may be supplemented to correct, to add additional information, to change the status or classification of a report, or to include comments regarding the details or investigation of an offense. However, tampering with, altering, or falsifying any report, document, or record is prohibited and may result in disciplinary action, up to and including termination.

L. Unless authorized by law, no deputy or civilian employee shall remove or destroy or cause the removal or destruction of any original report, document, or record without prior written authorization.

M. With the exception of an original report, document, or record which requires legal authorization for destruction, any document that contains sensitive information that can be misused for potential physical harm or financial fraud, such as personal identifiers and/or a person’s home address shall be shredded before being discarded. Such documents may include, but are not limited to, non-original copies of offense reports and supplements, officer’s notes, and personnel documents.

N. A subpoena may be issued to or otherwise received by a deputy or civilian employee to appear to testify, or to bring certain documents. The only person who can release a deputy or civilian employee from a subpoena is the judge of the court from which it was issued.

1. The City Solicitor accepts service to City of Philadelphia Employees for all duty related issues.

2. In the event a deputy or civilian employee is served with or otherwise receives in any manner a subpoena, the employee shall immediately notify their supervisor and present to the supervisor a copy of the subpoena, who shall then also notify the City Solicitor and the appropriate Deputy Chief via chain of command and the Deputy Chief, Internal Affairs.

3. Unless exigent circumstances exist, the employee will be personally served with the subpoena. If the employee is unavailable to accept the subpoena, only the employee’s supervisor shall accept on their behalf. Personnel in Internal Affairs shall be authorized to accept subpoenas on behalf of all officers. Before accepting a subpoena on behalf of any other Sheriff’s Office employee, the subpoenaed employee must be contacted to confirm the employee will be available to comply with the subpoena on the date and time the employee’s presence is requested.

4. When a deputy or civilian employee is served with or receives a subpoena duces tecum, which is a court order to a person to come and bring certain records and/or
files, the employee shall immediately deliver the original subpoena to the Captain, Internal Affairs and retain a copy for their own information.

a. No officer or civilian employee shall release any department records or evidentiary matters pursuant to a subpoena duces tecum without prior written approval from the Undersheriff.

b. Internal Affairs or Undersheriff shall be the only entities to release departmental records and/or files requested in a subpoena duces tecum.

5. Original documents will not be released unless specifically ordered by the judge presiding over the court involved; otherwise, only copies of documents shall be provided.

O. Deputies or civilian employees must be present or available to testify in any court or before any grand jury when officially notified by the Office chain of command or when subpoenaed to appear. In civil or criminal cases outside Philadelphia employees shall respond to a proper subpoena or the specific direction of the Sheriff, Chief Deputy, or Undersheriff.

P. Deputies or civilian employees who, for a valid reason, are unable to answer or otherwise respond to an official summons must immediately so notify the court, grand jury, or person causing the summons to be issued when they become aware of their inability to answer and prior to the time they are scheduled to appear. The reason for the request to be excused shall also be contemporaneously reported to the deputy’s or civilian employee’s supervisor.

Q. Court-Ordered Production of Documents or Evidentiary Items: In the event that an deputy or civilian employee receives service or notice of a court order requiring their presence in court on a particular date and time, and/or which requires the employee to bring certain items to court on a particular date and time, the employee named in the order shall immediately scan or photocopy the order and either email, Fax, or hand deliver a copy to Internal Affairs, who shall then coordinate with the Undersheriff. The employee named in the order shall make all necessary preparations to abide by the order and to be present in court or directed by the order. The employee shall also make all appropriate arrangements with Internal Affairs to secure or transport any items specified in the order to the court on the date and time specified.

R. No deputy or civilian employee shall give any lawyer, bail bond broker, private investigator, or any other person unauthorized information regarding prisoners in confinement, property in custody, property under the control or in the process at any stage of Sheriff’s Sale, or other records of the Office of the Sheriff.

S. No deputy or civilian employee shall reveal confidential information or documents to anyone unless authorized to do so and then only to a person or persons authorized to receive such confidential information.
T. Deputies or civilian employees shall not communicate:

1. Any information or documents relating to a Sheriff Sale without authorization of the Deputy Chief,

2. Or communicate any information which may facilitate persons accused of criminal acts to escape arrest or punishment or which may enable them to dispose of or secrete evidence of unlawful activity.

U. No deputy or civilian employee shall use any Office of the Sheriff file or utilize any computer terminal to examine or retrieve offense/incidents for personal means.

LXXXIV. PUBLIC ACTIVITIES

A. Public Activities / Rewards

1. No employee shall engage in any strike against the city/county government or actively participate in a strike against any other person, association of persons, agency, firm, corporation, the United States, the Commonwealth of Pennsylvania, or any political subdivision thereof.

2. No employee shall attempt to influence members of the Civil Service Commission, Sheriff’s Office, Mayor, City Council, City Government, Judicial System, or any other persons outside of the Sheriff’s Office for the purpose of obtaining any transfer, assignment, promotion, benefit, or favor.

3. Employees of the Office of the Sheriff shall not be permitted to take an active part in any political campaign of another for an elective position of the city if they are in uniform or on active duty. This shall prohibit such acts as making political speeches, passing out cards, or other political literature, writing letters, signing petitions, actively and openly soliciting votes, and making public derogatory remarks about candidates for such elective positions.

   a. No employee shall knowingly become a candidate for nomination or election to any public office unless in compliance with City of Philadelphia policy.

4. Members of the Sheriff’s Office shall not join or be members of any organization which has as its purpose the overthrow of, or interference with the established government, either by force or illegal means. Neither will members of the Office join organizations that advocate hatred toward any group, with specific reference to race, creed, color, gender, and religion.

5. No employee shall accept any gift for the purpose of influencing said employee in the performance of their duty, or as an inducement to favor the one offering the same.
6. No employee shall use their position in a manner designed to harass, belittle, intimidate, oppress, or influence any person, group, fraternal organization, club, or business.

7. Employees of the department shall not solicit, seek, or accept free or otherwise discounted food, drink, goods or services from any merchant or business establishment during the employee's performance of duty or by reason of them being employees of the Sheriff's Office.

8. No deputy shall display their badge or other identification while off-duty for the purpose of seeking free admission to any place of entertainment.

9. No employee, either directly or indirectly, shall attempt to influence the outcome of any Office disciplinary matter by using the social media, the newspaper or television unless in compliance with directives.

LXXXV. ETHICAL STANDARDS

A. No employee of the Office of the Sheriff shall knowingly:

1. Accept or solicit any gift or favor from any person, corporation, or association of persons that might reasonably tend to influence the member in the discharge of their official duties, or in consideration of such member having exercised any official power or having performed any official duty.

2. Accept or solicit any gift or favor, including a promise of future employment, or a favor or service from another member or any other person, corporation, or association of persons:
   a. Rendering services for which the employee is employed.
   b. The paying of fines, utility franchise or filing fees, and taxes; and
   c. Subject to restrictions contained in the Charter of the City of Philadelphia. Executing and performing any community facilities contract or plat in compliance with laws and regulations applicable to any person; provided, however, that if any city ordinance, rule or regulation allows any discretion by the appropriate officers or employees of the city in the interpretation or enforcement of such ordinance, rule or regulation, any such discretion shall be exercised in favor of the city in connection with any such community facilities contract or plat.

3. Appear before a city or body of which the employee is a part as a representative for any private person, group, or interest; or represent, directly or indirectly, any private person, group, or interest before any department, agency, commission or board of the City of Philadelphia.
4. Represent, directly or indirectly, any private person, group, or interest in any action or proceeding against the interests of the city or in any litigation in which the city or any department, agency, commission, or board thereof is a party. This section does not prohibit truthful testimony when an employee is subpoenaed for that purpose.

5. Represent, directly or indirectly, any other private person, group, or interest in any action or proceeding in State or Federal Courts, and the Municipal Courts of the City of Philadelphia that was instituted by a city officer or employee in the course of official duties, civil or criminal proceedings in which any city officer or employee is a material witness for the prosecution.

6. If any employee of the Office has a substantial interest, direct or indirect, in any individual or entity involved in any decision pending before such member or an official body, agency or commission to which the member has been appointed, the member shall not vote or otherwise participate in the consideration of the matter, but shall publicly disclose the nature and extent of such interest in the official records of the body, agency, or commission prior to any discussion or determination of the matter.

7. Employees shall not permit their name, photograph, or identities as employees of the Sheriff's Office to be used to endorse any product or service without prior written permission of the Sheriff or designee. Permission shall not be granted for personal or business profit.

8. Nothing in this section shall be construed to prohibit the acceptance by the department of donations of:

a. Money or items to be used for or in conjunction with ceremonies or appreciation events to honor employees of the department; or
b. Real property, equipment, or other items to be used by the Office of the Sheriff in the normal scope of business.

9. Employees have an obligation and responsibility to report all facts or credible information regarding any criminal activity by another employee or any serious breach of written directives.

10. No employee shall in any way cause or conspire to cause retaliatory action against any individual who has been involved in any such investigation as a defendant, complainant, witness, victim, investigator, or any other capacity.

BY ORDER OF:

[Signature]

SHERIFF DATE