ILLINOIS STATE POLICE DIRECTIVE
OPS-200, EVIDENCE – DEFINITIONS AND RESPONSIBILITIES

RESCINDS:	**REVISED:**
OPS-200, 2024-036, revised 11-12-2024	01-28-2026 **2026-007**
RELATED DOCUMENTS: ADM-001, ENF-016, ENF-028, EQP-015, EQP-016, OPS-057, OPS-101, OPS-200, OPS-201, OPS-202, OPS-203, SRV-003, SRV-005, All-Hazards Guide, Evidence Custodian's Manual	**RELATED CALEA STANDARDS (6th Edition):** 42.1.6, 42.2.1, 42.2.2, 42.2.3, 55.2.4, 61.1.10, 61.2.1, 61.2.2, 82.2.4, 82.2.5, 82.3.6, 83.2.1, 83.2.2, 83.2.3, 83.2.4, 83.2.5, 83.2.6, 83.3.1, 83.3.2, 84.1.1, 84.1.2, 84.1.3, 84.1.4, 84.1.5, 84.1.6, 84.1.7, 84.1.8

I. POLICY

The Illinois State Police (ISP) will establish guidelines to collect, preserve, package, document, and transfer evidence, property, and related items in a standard and consistent manner. Standardized definitions for use in the necessary evidence directives will be established.

II. DEFINITIONS

Unless otherwise noted, these definitions will apply to all instructions concerning evidence, property, or related items.

II.A. Annual audit – A review of evidence, handling procedures, records, disposition, and storage facilities (Refer to ISP Directive OPS-203, "Evidence – Inspection, Inventory, Retention, and Disposal.")

II.B. Barcoded Evidence Analysis Statistics and Tracking (BEAST) – an automated evidence management system maintained in a secure manner. (Refer to ISP Directive OPS-203, "Evidence – Inspection, Inventory, Retention, and Disposal.")

II.B.1. When secured in an evidence vault, evidence, property, and related items must be barcoded with a unique identifier and definition by the Evidence Custodian (EC) and entered into the system.

II.B.2. ECs will maintain a manual evidence log in the event the evidence vault is not equipped with BEAST, or when BEAST is temporarily inaccessible. Upon conversion of all items to BEAST, a manual log is no longer necessary but will be retained in a secure location for historical purposes.

II.B.3. ECs are mandated to follow the provisions of this directive, as well as those described in ISP Directives OPS-201 through OPS-203, and the Evidence Custodian's Manual regarding all evidence handling and processing.

II.C. Cloud Storage – secure, offsite data storage environments, approved by the Department of Innovation and Technology (DoIT), designed to store ISP digital evidence and other digital files.

II.D. Computer-related evidence (Refer to ISP Directive OPS-202, "Evidence – Collecting and Packaging Computer and Digital/Multimedia Forensic Evidence.")

II.D.1. Computer peripherals

II.D.1.a. Devices used with a computer for recording, storage, or retrieval of information.
II.D.1.b. Examples: diskette drives, fixed disk (hard) drives, zip drives, jaz drives, scanners, monitors, keyboards, mice, etc.

II.D.2. Electronic storage media – any data storage device (i.e., audio cassette tape, videotape, 8mm tape, CD, DVD, diskette, hard drive, thumb drive, or otherwise) used for the retention of digital files.

II.D.3. Computer Evidence Recovery – the procedures executed to find evidence or exculpatory material residing on computer systems, computer media, or computer peripherals. (Refer to

ISP Directive OPS-202, “Evidence – Collecting and Packaging Computer and Digital/Multimedia Forensic Evidence.”)

II.E. Court order – a written order issued by a judge authorizing the disposal (e.g., destroy, return to owner, etc.) of all or specific items of evidence. (Refer to ISP Directive OPS-203, “Evidence – Inspection, Inventory, Retention, and Disposal.”)

II.F. Department-approved storage facility – safe deposit boxes, garages, warehouses, or other facilities rented or borrowed to accommodate security or space needs when authorized by the Troop/Zone Commander or Metropolitan Enforcement Group (MEG)/Task Force (TF) Director, or designee, and the EC. The Statewide Evidence Vault (SEV) must be notified of approved facilities used for evidence storage, other than the Troop/Zone vault. (Refer to ISP Directive OPS-203, “Evidence – Inspection, Inventory, Retention, and Disposal.”)

II.F.1. Record-keeping responsibilities and security measures for high-value items are the same as for material stored in a department facility.

II.F.2. After vehicles, boats, and other large conveyances have been processed for evidentiary purposes, they may be stored in parking areas that are locked or may be parked at a troop headquarters that is occupied 24 hours a day. (Refer to ISP Directive ENF-016, "Tows.")

II.F.2.a. Vehicles awaiting processing by Scene and Evidence Services Command (SESC) will be secured and protected, which includes preventing persons from entering the vehicle as well as the removal of evidentiary items.
II.F.2.b. Due care will be taken to ensure all personal property is secure.
II.F.2.c. High-value items should be placed into an approved evidence vault after processing.

II.G. Digital evidence – a digital file stored as evidence.

II.G.1. Digital evidence must be stored on electronic storage media and secured in an evidence vault or transferred to a secure Cloud Storage environment using approved software.

II.G.2. Digital files output from digital or audio recording systems, obtained from parties as digital files sent via a computer network, or otherwise obtained independent of an original media, shall be stored in a department-approved digital evidence storage system.

II.H. Digital file – a block of data stored on, or independent of, computer media identified by a file name that is read by a computer or other device. Digital files include, but are not limited to, videos, audio files, images, documents, spreadsheets, text files, web pages, log files, or forensic copies of complete file systems.

II.I. Electronic evidence – tangible items of evidence such as computers, hard drives, or other computer/electronic storage media that may contain digital files.

II.J. Evidence – any objects, instruments, articles, digital files, or other items collected or seized by employees or investigating officers during the course of an investigation or pursuant to a search, including a search incident to arrest, that may have significance as a means of ascertaining the truth of any alleged matter of fact relevant to a crime or a criminal prosecution, except that related items as defined herein are not evidence for purposes of this policy. (Refer to ISP Directives, OPS-200 through OPS-203.)

II.K. Evidence Custodian (EC) – employee designated by the Troop/Zone Commander or MEG/TF Director to administer the operation of a Troop/Zone/MEG/TF Evidence Vault. The EC is not required to be a sworn officer. (Refer to this directive and ISP Directives OPS-201 through OPS-203.)

II.K.1. There will also be at least one Alternate Evidence Custodian (AEC) designated in each location.

II.K.2. References to ECs in this policy also apply to AECs.

II.L. Evidence Custodian's Manual – a procedures manual provided by the Statewide Evidence Custodian (SEC) for use by all ECs. This is a Specialty Manual containing written directives as defined in ISP Directive ADM-001, "Manuals and Directives." (Refer to this directive and to ISP Directive OPS-203, "Evidence – Inspection, Inventory, Retention, and Disposal.")

II.M. Forensic evidence – any evidence in the Department's possession or control that is reasonably likely to contain forensic evidence, including, but not limited to, fingerprints or biological material secured in relation to a trial. Biological material includes, but is not limited to, blood, hair, saliva, or semen from which genetic marker groupings may be obtained. (Refer to ISP Directives OPS-202, "Evidence – Collecting and Packaging Computer and Digital/Multimedia Forensic Evidence," and OPS-203, "Evidence – Inspection, Inventory, Retention, and Disposal.")

II.N. Hazardous material – a substance or combination of substances that, because of its concentration, chemical, physical, or infectious characteristics is capable of posing an unreasonable risk to health and safety or may cause injury or death. (Refer to ISP Directive OPS-201, "Evidence – Collecting and Packaging.")

II.O. Hazardous materials incident – any release, intentional or unintentional, of a hazardous material from containment in any quantity from a vehicle, fixed facility, or lost/unattended package. (Refer to ISP Directive OPS-201, "Evidence – Collecting and Packaging.")

II.P. Hazardous waste – a waste product or combination of substances that, because of its concentration, chemical, physical, or infectious characteristics is capable of posing an unreasonable risk to health and safety or may cause injury or death and has been identified by law, regulation, or rule as posing a risk to public health or the environment. (Refer to ISP Directive OPS-201, "Evidence – Collecting and Packaging.")

II.Q. High-value items – exceptional, valuable, or sensitive items of high value such as: (Refer also to ISP Directive OPS-201, "Evidence – Collecting and Packaging.")

II.Q.1. All firearms

II.Q.2. All drugs

II.Q.3. All cash

II.Q.4. All jewelry

II.Q.5. Evidence, property, and related items, except vehicles and other conveyances, with a value of $500 or more. (See paragraph II.F.2.c. of this directive.)

NOTE: Cellular phones and tablets seized as evidence that are pending a digital forensic extraction and/or transfer to the Digital Crimes Unit may be stored in a secure location or a temporary storage locker to maintain power to the device. (Refer to ISP Directives OPS-201, "Evidence – Collecting and Packaging," and OPS-202, "Evidence – Collecting and Packaging Computer and Digital/Multimedia Forensic Evidence.")

II.R. Inspection – a review of evidence, handling procedures, records, disposition, and storage facilities. (Refer to ISP Directive OPS-203, "Evidence – Inspection, Inventory, Retention, and Disposal.")

II.S. Integrity Packaging – the combined packaging of exhibits from a single case into a larger container to maintain the integrity of the evidence by reducing its excessive handling. Integrity packaging is allowed at the SEV. Integrity packaging is also allowed at Field Vaults if the following criteria are met:

II.S.1. The EC's command determined the case being placed into integrity packaging requires storage for a long or indefinite time period (Code 14 status).

II.S.2. The EC has requested and received approval from the SEC, or designee, to integrity package the case.

II.S.3. The Primary EC and a supervisor in their chain-of-command ranked Master Sergeant or above will follow the procedures for Integrity Packaging Evidence as outlined in the Statewide Evidence Vault (SEV) Operations Manual. The two officers sealing the exhibits within the box are responsible for ensuring the contents within the integrity package are correct.

NOTE: Refer to ISP Directives OPS-201 through OPS-203.

II.T. Inventory – an accounting of evidence, property, and related items using BEAST, if available, to ensure vault items are in the correct location and all vault items are present. (Refer also to ISP Directive OPS-203, "Evidence – Inspection, Inventory, Retention, and Disposal.")

II.T.1. Change of custodian inventory – conducted upon assignment or relief from assignment as an EC prior to the custodian's departure.

II.T.2. Change of facility inventory – conducted whenever the location of a storage facility is changed.

II.U. Mobile device – a hand-held electronic device providing a touchscreen interface with digital or physical buttons, including, but not limited to, a tablet, cellular phone, smart phone, or GPS unit. Many such devices connect to the internet via Wi-Fi, Bluetooth, or cellular networks. Mobile devices may run mobile operating systems that allow third-party applications to be installed and run. Mobile devices may also require user authentication, such as use of a passcode and/or biometrics, such as facial or fingerprint identification.

II.V. Overhear tapes or other recordings – recordings of conversations made pursuant to 725 ILCS 5/108A-3 or other court authorized interception. (Refer to ISP Directive OPS-203, "Evidence – Inspection, Inventory, Retention, and Disposal.")

II.W. Physical evidence – tangible items of evidence collected or seized during the course of an investigation.

II.X. Property – tangible instruments, articles, items, or other objects that come into the possession of the Department by means other than a search. (Refer to ISP Directives OPS-200 through OPS-203.)

II.X.1. Property includes:

II.X.1.a. Abandoned property – property left by the owner intending to relinquish all rights thereto
II.X.1.b. Lost/Found/Personal property – property unintentionally separated from its owner's dominion
II.X.1.c. Stolen property – property over which control has been obtained by theft
II.X.1.d. Otherwise illegally possessed property – property that is unable to be legally possessed
II.X.1.e. Related items – reports, records, receipts, photographs, negatives, audiotapes, videotapes, and other similar items obtained during the course of an investigation but are not likely to be used as evidence in litigation. (Refer to ISP Directives OPS-201 through OPS-203.)

II.X.2. Exceptions:

II.X.2.a. Overhear tapes
II.X.2.b. Audio and video recordings, photographs, and negatives of confessions, photo lineups, surveillance, or other events that have probative value
II.X.2.c. Video media from in-car cameras (Refer to ISP Directive EQP-015, "Law Enforcement Mobile Recording Equipment (LEMRE).")

II.Y. Secure location – a storage location in a troop or zone headquarters designed to ensure adequate safekeeping and record keeping of related items as well as cellular phones and tablets seized as evidence that are pending a forensic digital extraction and/or transfer to the Digital Crimes Unit. (Refer to ISP Directives OPS-201, "Evidence – Collecting and Packaging," and OPS-203, "Evidence – Inspection, Inventory, Retention, and Disposal.")

II.Z. Securities – currency and/or documents readily convertible to cash such as travelers checks and money orders. (Refer to ISP Directives OPS-201, "Evidence – Collecting and Packaging," and OPS-203, "Evidence – Inspection, Inventory, Retention, and Disposal.")

II.AA. Statewide Evidence Custodian (SEC) – SEV employee designated by the Deputy Director of the DFS to administer and operate the SEV and storage facilities. The SEC also provides functional supervision over the Department's evidence program and all Troop/Zone/MEG/TF Evidence Vaults, and whose approval must be obtained prior to destruction of evidence/property. References to the SEC in evidence directives also apply to assistant SECs (except for the selection process of assistant SECs). (Refer to ISP Directives OPS-200 through OPS-203.)

II.BB. Statewide Evidence Vault (SEV) – a highly secure storage facility located in Springfield, Illinois, under the direct supervision of the SEC. (Refer to ISP Directive OPS-203, "Evidence – Inspection, Inventory, Retention, and Disposal.") All evidence maintained at the SEV will be stored only at the Enhanced Security level. (See II.DD.8.b. of this directive and the **NOTE** below in II.BB.4.) The SEV will serve as the designated evidence vault for the ISP work units in the Springfield area. In addition, the SEV and storage facility may be used by any division and will provide storage for Troop/Zone/MEG/TF Evidence Vaults for:

II.BB.1. Evidence that must be retained for an extended time

II.BB.2. Evidence requiring enhanced security over the level normally available at Troop/Zone/MEG/TF Evidence Vaults

II.BB.3. Bulky items of evidence

II.BB.4. Evidence requiring special handling

NOTE: Security at the SEV is comprised of the following levels:

Level 1: Exterior building access limited to certain ISP personnel.
Level 2: Evidence vault security door access limited to SEV personnel only.
Level 3: Enhanced evidence vault security limited to SEV personnel only.
Level 4: Secured secondary vault located within the enhanced vault security area limited to SEV personnel only.

II.CC. Temporary storage – a drawer, cabinet, safe, room, etc., at an official facility that can be locked, or the trunk of an official ISP vehicle. Only the person storing the material will have a key or combination to the temporary storage area. (Refer to ISP Directives OPS-201, "Evidence – Collecting and Packaging," and OPS-202, "Evidence – Collecting and Packaging Computer and Digital/Multimedia Forensic Evidence.")

II.DD. Troop/Zone Evidence Vaults – receiving and storage facility space designated by, and under the direct control of, the respective division's patrol/investigations headquarters and offices of other units, as deemed necessary by the appropriate Deputy Director, including MEGs and TFs. (Refer to ISP Directives, OPS-201 through OPS-203.)

II.DD.1. The Forensics Sciences Command laboratories are receiving facilities but are to be considered storage facilities only for the length of time necessary to complete the required analysis.

II.DD.1.a. A high-level of security and specialized capabilities, such as refrigeration, are required at these facilities.

II.DD.1.b. The Deputy Director of the Division of Forensic Services (DFS) may authorize an exemption to the receipting and logging procedures specified in this directive in special or unusual circumstances.

II.DD.2. Crime Scene Services (CSS) offices and vehicles equipped with secure evidence storage lock boxes can serve only as temporary storage areas for evidence being processed by Crime Scene Investigators (CSIs). When CSS officers transfer evidentiary exhibits to any permanent storage facility/evidence vault, the CSS officer must follow the same processing

procedures as any other submitting officer prior to placing the evidence into permanent storage.

NOTE: CSS will abide by CSS Directives regarding the handling and processing of evidence.

II.DD.3. Digital Crimes Unit (DCU) evidence vaults and processing laboratories are receiving facilities for computer-related evidence only and are to be considered storage facilities only for the length of time necessary to complete the required analysis.

II.DD.3.a. A high level of security with a controlled/protected environment and immediate access to specialized computer processing equipment and forensic analysis software are required at these facilities.

II.DD.3.b. The Deputy Director of the Division of Forensic Services (DFS) may authorize an exemption to the receipting and logging procedures specified in this directive in special and unusual circumstances.

II.DD.4. In locations where units of more than one division share a building, there may be a single, cooperatively administered and operated receiving and storage facility. Furthermore, units within divisions that do not operate an evidence vault within the Troop will use a locally available Troop/Zone Evidence Vault.

II.DD.5. Drop lockers are storage spaces accessible for deposit of evidence/property when ECs are not available and from which only the EC may remove the material. Each Troop/Zone Evidence Vault will provide drop lockers for use by officers submitting evidence to the vault when the EC is unavailable. Evidence, property, and related items placed in a drop locker must, within seven calendar-days, be entered into BEAST and secured in the vault or taken to a laboratory. (Refer to ISP Directives OPS-201, "Evidence – Collecting and Packaging," and OPS-202, "Evidence – Collecting and Packaging Computer and Digital/Multimedia Forensic Evidence.") All evidence, property, and related items secured in a drop locker must be entered into BEAST by an EC prior to transferring it back to an officer or relocating it to another Troop/Zone evidence vault or lab.

II.DD.5.a. Drop lockers should be adequate in number and size to handle long guns and other evidence normally brought to such a facility.

II.DD.5.b. Evidence must be properly marked and packaged before personnel place it in a drop locker.

II.DD.5.c. Drop lockers shall be securely fastened to the wall or floor within the facility.

II.DD.5.d. Each drop locker shall have an attached BEAST generated label designating the locker as a drop locker, with the drop locker's assigned number.

II.DD.5.e. All drop lockers will be listed as storage locations within BEAST.

II.DD.5.f. Drop lockers are not considered temporary storage areas and will not be used as such.

II.DD.6. If a MEG/TF unit wants to maintain a drop locker, the unit must appoint an Alternate Evidence Custodian (AEC) to relay evidence from the MEG/TF drop locker to the Troop/Zone vault responsible for the storage of that unit's evidence. All evidence removed from the drop locker by MEG/TF AECs will be taken to the responsible vault and properly entered into BEAST on the same day the evidence was removed from the drop lockers.

II.DD.7. Troop/Zone Evidence Vaults will provide evidence storage for any ISP unit located within the Troop/Zone when that unit does not operate an evidence vault of its own and requires evidence storage services.

II.DD.8. Troop/Zone Evidence Vaults will provide:

II.DD.8.a. Physical security, including a functioning intrusion detection alarm system.

II.DD.8.b. Enhanced security within the vault (e.g., safe or locked cabinet) for high-value items. Troops/Zones unable to provide enhanced security due to restricted vault space may show compliance with enhanced security measures by installing a

second, locking, controlled access door in combination with the existing vault door. The second door may consist of a chain link design.

II.DD.8.c. A properly designed and functioning ventilation system.

II.DD.8.d. Adequate space based on units served.

NOTE: Drop lockers are **not** temporary storage areas.

III. RESPONSIBILITIES

III.A. Employees are responsible for:

III.A.1. The security of evidence, property, and related items in their possession.

III.A.2. Proper packaging of evidence, property, and related items submitted to a laboratory or evidence vault.

III.A.3. Proper documentation on the evidence package.

III.A.4. Proper documentation in ISP reporting software and all applicable evidence transfer forms to record chain-of-custody of each item of evidence.

III.B. Division of Patrol (DOP) and DCI Region Commanders will ensure that inspections of evidence, evidence handling procedures, records, and evidence dispositions at storage facilities under their command are conducted.

III.C. DOP and DCI Region Commanders will ensure Troop/Zone Commanders and the MEG/TF Directors identify all evidence eligible to be disposed of (semi-annually) through evidence disposal worksheets provided by the EC.

III.D. The Troop/Zone Commander or the MEG/TF Director, where a Troop/Zone/MEG/TF Evidence Vault is located, is responsible for:

III.D.1. Ensuring that inspections are completed as prescribed in ISP Directive OPS-203, "Evidence – Inspection, Inventory, Retention, and Disposal."

III.D.2. Ensuring a supervisor not routinely or directly connected with control of property conducts an annual audit of property held by the Agency. The Troop/Zone Commander of MEG/TF Director will appoint this person.

III.D.3. Ensuring an alarm system is installed, tested and maintained:

III.D.3.a. The alarm system will be separate from the building alarm system so it may remain active when the building alarm system is deactivated.

III.D.3.a.1) Only the EC can activate or deactivate the alarm systems. Anytime someone other than the EC resets the alarm, that person will immediately notify the EC.

III.D.3.a.2) Only the EC will have access to the keys or codes that access the evidence vault.

III.D.3.a.3) Troop/Zone Commanders and MEG/TF Directors will ensure that access keys and/or codes for Troop/Zone/MEG/TF Evidence Vault doors and alarms are changed whenever the custodian and/or AEC changes. The Troop/Zone Commander and MEG/TF Director must receive written authority from the SEC in order to change only the alarm access (and not the locks).

III.D.3.a.4) Alarm testing will be conducted whenever an inspection or inventory is conducted.

III.D.3.b. In a facility staffed 24 hours per day, the system may notify department personnel (e.g., ring in the Communications Center or advise the Operations staff).

III.D.3.c. In facilities not staffed 24 hours per day, the system will be linked to an outside monitoring entity that will notify the nearest police agency or ISP Telecommunications Center to secure the site until a custodian arrives to assess the situation.

III.D.3.d. Alarm tests conducted whenever inspections or inventories are completed will be noted in the inspection or inventory report.

III.D.4. Reviewing and evaluating a response plan at least annually.

III.D.5. Promptly notifying the SEC of any changes to the EC or AEC.

III.D.5.a. Notification will be in advance, if feasible, to allow time for training the new EC prior to assuming the EC duties.

III.D.5.b. The SEC will remove the security clearance for the vacating EC.

III.D.6. Consulting with the SEC in all matters pertaining to evidence/property control, including construction of evidence vault, security matters, etc.

III.D.7. Ensuring case officers identify all evidence eligible to be disposed of (semi-annually) through evidence disposal worksheets provided by the EC.

III.D.8. Ensuring the EC develops and implements controls consistent with ISP policy to properly receive, document, and return evidence that may be placed into a Troop/Zone/MEG/TF evidence vault and/or drop lockers by an outside agency or department.

III.E. Troop/Zone/MEG/TF ECs will:

III.E.1. Require proper marking and packaging on incoming evidence/property.

III.E.2. Obtain and approve storage space for unusual needs beyond the capacity of existing facilities.

III.E.3. Ensure that no dangerously explosive substance or hazardous materials are stored in departmental facilities.

III.E.3.a. Forensic Science Command Laboratories may store limited amounts of explosives or other hazardous materials, i.e., flammables necessary to conduct analysis of evidence submitted to serve as comparative standards.

III.E.3.b. Fireworks categorized as class “C,” novelty,” or 1.4G UN0336 consumer fireworks may be handled as routine evidence and stored in department evidence facilities.

III.E.3.c. Proper storage for fireworks other than class “C,” “novelty,” or 1.4G UN0336 consumer fireworks will be coordinated with the SEC.

III.E.3.d. Refer to ISP Directive OPS-101, “All-Hazards Operations,” and the All-Hazards Guide for information regarding explosives and ISP Directive OPS-057, “Hazardous Materials Incidents,” for information regarding hazardous materials.

III.E.4. Initiate and maintain required records and files (notifying officers’ supervisors when packaging, labeling, or record cards need to be corrected).

III.E.5. Be aware of the needs of victims and witnesses and assist the investigating officer in returning evidence/property to its rightful owner(s) as soon as feasible.

III.E.6. Review the documentation, prepare for disposal of evidence/property in accordance with this directive and department procedures, and notify the SEC when evidence/property is ready to be destroyed.

III.E.7. Participate in all required inspections including change of custodian inventory upon assignment or relief of assignment as EC.

III.E.8. Have the option to deliver or pickup evidence from a court, laboratory, or other location (the EC will not accept improperly packaged or labeled items).

III.E.9. Ensure all evidence transfers are for appropriate reasons, i.e., court, forensic testing, long-term storage, disposal, etc., and documented with a signed evidence receipt printed from the BEAST or on an Evidence Inventory and Receipt form (ISP 1-010).

III.E.9.a. Evidence in active cases cannot be removed from the vault to be used as props in facilitating other cases.

III.E.9.b. Court orders must be obtained authorizing the Department to keep evidence instead of disposing of it.

III.E.9.c. Evidence held for enforcement purposes, i.e., reverse role, props, must be transferred to the SEV for storage upon adjudication of the case and issuance of the court order.

III.E.10. Provide proper packaging materials along with training to officers submitting evidence, property, and related items to the evidence vault.

III.E.11. Ensure copies of Troop/Zone/MEG/TF Evidence Vault inspections are forwarded to the SEC within five working-days.

III.E.12. Manage the evidence in the vault by providing evidence disposal worksheets (semi-annually) to the case officer(s) identifying all evidence eligible to be disposed.

III.E.13. Complete and maintain the Evidence Vault Annual Checklist Form (ISP 4-162).

III.E.14. Establish a written response plan that will ensure:

III.E.14.a. The appropriate Communications Center(s) responsible for responding to the alarm are provided with a current list of appropriate operations and evidence vault personnel's phone numbers to contact in the event an alarm is activated.

III.E.14.b. The current name and phone number of the alarm company responsible for the alarm system is on file at the site of the evidence vault.

III.E.14.c. Representatives of the alarm company are aware of the requirement of providing positive identification prior to accessing the system.

III.E.14.d. When, where, and how the evidence vault will be secured and relocated if the evidence vault security is breached due to manmade or natural disaster. This recovery plan may be separate or included in the facility recovery plan.

III.E.15. Evidence vault access

III.E.15.a. Only ECs in charge of a particular evidence vault are permitted unaccompanied and unrecorded access to the evidence vault.

III.E.15.b. The EC, the Troop/Zone Commander, or the MEG/TF Director will grant access to other persons on an as-needed basis. The EC must accompany persons allowed access.

III.E.15.c. The EC is responsible for documentation of access:

III.E.15.c.1) The date and time of access/exit, the name and signature of person entering, and the purpose for access must be documented.

III.E.15.c.2) The EC who accompanies the person will also provide a signature on the log.

III.E.16. Evidence lost or unable to be located

III.E.16.a. Evidence that is lost or unable to be located will be reported to the Troop/Zone Commander or MEG/TF Director and the SEC by the EC prior to the end of the shift in which this was discovered.

III.E.16.a.1) The Troop/Zone Commander or MEG/TF Director will determine what steps should be taken to try to locate the evidence and notify DII and the SEC if the evidence is not located by the end of the work day in which it was discovered missing.

III.E.16.a.2) The SEC will notify the Commander of the Scene and Evidence Services Command.

III.E.16.b. If the evidence is located, the EC should notify their command, the SEC, and update BEAST, and if appropriate, return the item to its designated location.

III.F. The SEC will:

III.F.1. Provide functional supervision over the Department's evidence program and all Troop/Zone/MEG/TF evidence vaults and ECs. The SEC reports to the Scene and Evidence Services (SES) Commander.

III.F.2. Receive and review Troop/Zone/MEG/TF vault inspection reports.

III.F.3. Maintain a copy of the emergency response plan for all vaults.

III.F.4. Provide training, guidance, and feedback to Troop/Zone/MEG/TF vaults.

III.F.5. Serve as a resource to the ECs for assistance in the field and with BEAST.

III.F.6. Monitor physical conditions of evidence vaults and report any unsafe conditions to the Troop/Zone Commander or MEG/TF Director responsible for that evidence vault and the SES Commander.

III.F.7. Operate the SEV and approved storage facilities in accordance with the provisions in this directive.

III.F.8. Maintain contraband for use in reverse role operations.

III.F.9. Ensure evidence, property and related items are properly destroyed and all associated documentation is completed.

III.F.10. Create, administer, and maintain the procedures set forth in the EC's Manual.

III.F.11. Maintain procedures for proper handling, maintenance, and inspection of integrity packaging.

III.F.12. Maintain an evidence supply inventory for all Troop/Zone/MEG/TF vaults and allocate such supplies as requested.

Indicates new or revised items.

-End of Directive-