Virginia Department of Corrections

Authority, Inspection, and Auditing

Operating Procedure 030.1

Evidence Collection and Preservation

Authority:
Directive 030, *Audits and Investigations*

Effective Date: November 1, 2021

Amended: 4/1/22, 4/17/25

Supersedes:
Operating Procedure 030.1, July 1, 2018

Access: ☐ Restricted ☒ Public ☐ Inmate

ACA/PREA Standards:
5-ACI-3A-42, 5-ACI-3C-08, 5-ACI-3D-17;
4-ACRS-2C-03; §115.21, §115.221

Content Owner	Yulonda Wyche Security Program Coordinator	*Signature Copy on File* Signature	9/29/21 Date
Reviewer:	Randall C. Mathena Director of Security and Correctional Enforcement	*Signature Copy on File* Signature	9/29/21 Date
Signatory:	A. David Robinson Chief of Corrections Operations	*Signature Copy on File* Signature	9/29/21 Date

REVIEW

The Content Owner will review this operating procedure annually and re-write it no later than three years after the effective date.

The content owner reviewed this operating procedure in October 2022 and determined that no changes are needed.

The content owner reviewed this operating procedure in October 2023 and determined that no changes are needed.

The content owner reviewed this operating procedure in December 2024 and determined that no changes are needed.

COMPLIANCE

This operating procedure applies to all units operated by the Virginia Department of Corrections. Practices and procedures must comply with applicable State and Federal laws and regulations, ACA standards, PREA standards, and DOC directives and operating procedures.

Table of Contents

DEFINITIONS

Chain of Custody - The series of documented links between the time the evidence was obtained until presented in Court or other use and continuing to final disposition; the links are persons who handled the evidence, and where and when they did so.

Contraband - Any unauthorized item prohibited or excluded by law, rules, regulations, conditions, instructions, or any authorized item in excess of approved amounts

Evidence - The available body of facts or information indicating whether a belief or proposition is true or valid; evidence may include personal testimony, physical objects, documents, results from tests or analyses, audio/video recording, digital data, or any other form.

Special Operations Unit - The organizational unit within the Department of Corrections that serves as the mechanism for the statewide collection, assessment, and analysis of intelligence information, to include but not limited to gang-related material and dissemination to all appropriate stakeholders

PURPOSE

This operating procedure provides guidance for the proper collection, documentation, control, preservation, and disposal of all types of evidence within the Department of Corrections (DOC).

PROCEDURE

I. Evidence

A. This operating procedure provides a uniform protocol for the preservation, control, and disposition of all physical, digital, recorded, electronic, and other evidence obtained in connection with a violation of standards of conduct, law, facility rules, or conditions of supervision. All aspects of collection, documentation, chain of custody, preservation, and disposal of evidence will be addressed. (5-ACI-3A-42, 5-ACI-3D-17; 4-ACRS-2C-03; §115.21[a., b], §115.221[a., b])

B. Each facility and P&P District will designate an employee to serve as the Evidence Manager to oversee secure storage of evidence for their unit.

C. Each facility and P&P District will designate a secure evidence storage space for that unit.

1. Physical evidence must be stored in a safe or other such locked area with restricted access and each item placed into or removed from the designated secure evidence storage space must be documented.
   a. Only designated staff members are authorized to possess the combination or key to the secure evidence storage area and have access to the secure evidence storage area.
   b. A logbook must be kept in each secure evidence storage area. Any person opening the secure evidence storage area will make an entry in the logbook recording their name, the date and time of the opening, and a brief description of any item placed in or removed from the storage area.
   c. Each entry into the secure evidence storage space will be documented in the secure evidence storage log indicating; date and time of entry, name and title of employee making access and reason for access.
2. Each facility will be provided a designated digital storage folder accessible through the DOC network for storage of audio/video recordings and other digital evidence.

D. Principle types of evidence:

1. Contraband seized from an inmate/probationer/parolee, visitor, staff, or found on DOC property
2. Hardcopy documents
3. Reports of chemical or laboratory tests
4. Forensic physical or trace evidence collected from a victim or crime scene
5. Audio and/or video recordings
6. Digital evidence - computer files or data storage media
7. Electronic

E. Reports related to investigations, incidents, disciplinary actions (staff or inmate/probationer/parolee), or legal action should include a description of any relevant evidence and the disposition of that evidence. (5-ACI-3C-08)

II. Physical Evidence

A. Any contraband discovered, such as weapons, ammunition, explosives, illegal drugs, evidence of gang activity, mobile devices, and other material involved in an official investigation should be considered evidence.

1. In facilities, any officer or other employee discovering this type of evidence must immediately contact the Shift Commander, who will contact the designated Evidence Manager. The Office of Law

Enforcement Services will be notified in accordance with Operating Procedure 038.1, *Reporting Serious or Unusual Incidents*, when drugs or weapons are found.

2. In P&P Districts, contraband related to a probationer/parolee that may be used as evidence should be turned over to law enforcement officers for handling and storage whenever practicable; see Operating Procedure 910.1, *Probation and Parole Office and Staff Safety and Security*. If evidence must be retained in a P&P District, it will be documented and placed in the control of the designated Evidence Manager in accordance with this operating procedure.

B. When an item of physical evidence is discovered, the individual employee discovering the item will document the date, time, and location the item was discovered. As soon as practicable, this information will be entered on an *Evidence Custody Report* 030_F13.

1. If the Office of Law Enforcement Services or law enforcement will be investigating, the evidence should be left in place and the area secured as a crime scene if practicable; see the *Crime Scene Integrity* section of this operating procedure.
2. The employee who originally discovers the item of evidence should maintain complete control of the item.
3. The discovering employee will not pass the item of evidence to another employee for inspection and it must remain in the possession or control of the discovering employee at all times until it is turned over to the appropriate investigator or other authority.

C. If the employee discovering the evidence needs to transfer the evidence to another individual, the discovering employee must document the transfer on an *Evidence Custody Report* 030_F13 with the date, time, and signature of the receiving individual in the *Chain of Custody* section.

D. All items of evidence should be placed in an evidence container, sealed, and stored in the following manner:

1. The employee must clearly label the container with the name of the employee discovering the evidence, name of suspect/victim, reason for collection of the evidence, description of the evidence, location of discovery, and the date and time. All mobile devices will be wrapped in aluminum foil. *Caution*: Weapons or other items, from which fingerprints may be detected, should not be stored in plastic bags.
2. The bag, envelope, or container should be sealed by the employee discovering the evidence with their initial on the seal of the container. Each flap and seam of the envelope should be sealed with clear transparent tape.
3. All properly sealed evidence containers and *Evidence Custody Reports* will be given personally to the appropriate Evidence Manager as soon as possible with the transfer documented in the *Chain of Custody* section.
4. If kept at the facility or P&P Office, the evidence and related *Evidence Custody Report* should be placed in the designated secure evidence storage space.
   a. If an evidence safe is not available or suitable to the evidence item, the evidence should be placed under lock in a secure evidence storage area where only designated staff members may have access.
   b. The item should be left there until turned over to the DOC Special Operations Unit or Office of Law Enforcement Services, used in Court, or the case has otherwise been resolved.
5. Employees should handle evidence with extreme care to prevent evidence from becoming contaminated and to prevent injury. When practical, gloves should be worn to handle evidence and evidence should not be moved until a proper evidence container is available.
6. Evidence related to any investigation conducted by the DOC Special Operations Unit or Office of Law Enforcement Services should be held as per this operating procedure and handled as directed by the DOC Special Operations Unit or Office of Law Enforcement Services.

E. Physical evidence not suitable for designated secure evidence storage spaces

1. Alcohol discovered within the facility, other than that involved in an investigation, must be destroyed under supervision of two employees and a record maintained of such destruction.
2. All illegal drugs other than alcohol, or other material involved in an official investigation, must be turned over to the Office of Law Enforcement Services, local or state police, or, upon a Court order, destroyed in an appropriate manner by facility personnel and a record of the transaction maintained.
3. Over-sized items that do not fit into designated secure evidence storage spaces or evidence containers may be tagged and placed in a secure location.
4. Perishable evidence items (such as food) may be photographed or documented by written description on a *Disciplinary Offense Report* or *Internal Incident Report*. The Evidence Manager may then authorize disposal of the perishable evidence.

III. Digital Items and Audio/Video Recordings as Evidence

A. Each facility is provided a digital storage folder on the DOC network for secure storage of digital documents and audio video recordings that may be needed as evidence. This folder is suitable for storage of:

1. Camera recordings and video clips related to incidents
2. Recordings of inmate/probationer/parolee telephone calls
3. Digital photographs of evidence
4. Incoming or outgoing inmate secure messages
5. Any other evidence suitable for storage in a digital format

B. Management of Digital Storage Folders

1. Digital evidence will be given a file name consisting of the facility name abbreviation, date of the incident, inmate/probationer/parolee number, and a sequential number added if there are multiple files related to the same inmate/probationer/parolee on the same date.
   a. File name example - WRSP041518_1234567-2 is a recording made at Wallens Ridge State Prison on April 15, 2018. It is the second recording on this date related to inmate/probationer/parolee number 1234567 (this may be 2 different incidents or 2 different recordings of the same incident).
   b. Inmate/probationer/parolee number 9999999 may be used if no inmate/probationer/parolee is identified with the incident.
2. Files should be uploaded onto the facility's designated digital storage folder immediately after the incident is concluded. The successful upload must be confirmed before the recording is erased from the camera or other data storage device.
3. The file name(s) will be listed in the related *Internal Incident Report*, *Disciplinary Offense Report*, or *Incident Report*. The recording will not be attached to the *Report*.

C. Digital Storage Folder Access

1. Access to facilities' designated network storage folders is available to authorized users only. Approved users will receive confirmation and connection details from the Information Technology Unit (ITU) Security and the Security Operations and Emergency Preparedness Administrator. All access requests must be submitted on the *Digital Storage File Access* 030_F14; requests submitted in any other manner will not be approved.
2. Access to each facility's digital storage folder will be limited to designated facility staff as requested and approved by the Facility Unit Head on the *Digital Storage File Access* 030_F14.
3. A separate *Digital Storage File Access* 030_F14 will be completed for each request for staff access and must be submitted to the Regional Administrator and forwarded to the Security Operations and

Emergency Preparedness Administrator for final approval and assignment by ITU Security.

4. Levels of access to files on the facility's digital storage folder will vary depending on operational needs and may include:
   a. Read Files Access - i.e., Auditors
   b. Read & Execute Access (View) - e.g., Department Duty Officers, Regional Duty Officers, Office of Law Enforcement Services, others as designated by the Facility Unit Head i.e., Administrative Duty Officers
   c. Read & Write Files Access (Copy, Save, Send Files) - e.g., Institutional Investigator, Intelligence Officer
   d. Delete Files - ITU staff only with written approval of Security Operations and Emergency Preparedness Administrator
      i. Requests for the deletion of files from a facilities' Digital Storage Folder must be submitted in writing to the Security Operations and Emergency Preparedness Administrator.
      ii. The Security Operations and Emergency Preparedness Administrator will review the request and if approved, the written request will be forwarded to ITU Security as authorization to delete the file.
   e. Remove Access - ITU staff only with approval of Security Operations and Emergency Preparedness Administrator
5. The Regional Administrator will request access for Regional Office staff utilizing the *Digital Storage File Access* 030_F14 submitted to the Security Operations and Emergency Preparedness Administrator for final approval and assignment by ITU Security.
6. All other requests for access must be submitted on the *Digital Storage File Access* 030_F14 to the Security Operations and Emergency Preparedness Administrator for approval and assignment by ITU Security.
7. Copies of files may be provided to law enforcement and other non-DOC agencies only with the approval of the relevant Deputy Director or designee.
8. Cameras and data storage media must be carefully controlled and secured at all times to prevent unauthorized access to and misuse of digital evidence.

D. If a grievance is received that references a specific audio or video recording, a copy of the recording must be saved in the digital storage folder.

E. When an investigation is conducted, the digital evidence must be made available to the investigative unit and must become part of the investigation file.

F. The digital evidence must be retained for at least five years after the date of the incident.

G. If a lawsuit is filed or an investigation is in progress, the digital evidence must be retained until the investigation or lawsuit is completed.

IV. Cell Phones

A. This section provides guidance for seizing or collecting a cell phone or other digital device to be submitted to the Special Operations Unit for data extraction.

B. When a device is seized or collected, facility staff will consult with the Office of Law Enforcement Services Point of Contact to determine if OLES involvement is necessary.

1. If OLES involvement is necessary, a search warrant may be necessary for data extraction as determined by the OLES Agent or Supervisor.
2. If OLES involvement is not necessary, the device must be mailed or hand delivered to the Intelligence Analyst with OLU.

C. If the device is seized or collected from an inmate/probationer/parolee, employee, visitor, or civilian, the employee will:

1. Ask them for any charging cords or data cables related to the device.
2. Ask them for the passcode. Using the equipment available, some passcode protected devices can not be accessed without the passcode.

D. Staff should not attempt to manipulate or view the data on the device by utilizing the passcode. Any viewing or manipulation of the data on the device may require a search warrant and have to be explained later in Court.

E. The employee who seized or collected the device will secure the device and any accessories in an evidence bag or envelope in the same manner as all other physical evidence.

1. Leave device in original state and wrap in aluminum foil immediately.
2. Note the date, time, and location of the seizure for chain of custody purposes.

F. The appropriate investigator (OLES Agent, Intelligence Analyst with OLU, or Institutional Investigator) should take charge of the sealed evidence container for secure handling.

1. To request data extraction, staff should complete a *Device/Memory Card Seizure* 030_F20.
2. The device, a completed *Device/Memory Card Seizure* 030_F20, and *Evidence Custody Report* 030_F13should be given to the OLES Agent, Intelligence Specialist with OLU, or mailed to the Special Operations Unit, Attn: Cell Phone Extraction Request, 3525 Woods Way, State Farm, Va. 23160 via Certified Mail - Return Receipt Requested. The Return Receipt is proof that the phone was delivered for chain of custody purposes.

G. The Intelligence Analyst with OLU conducting the data extraction will provide findings to the appropriate investigator(s) as needed.

V. Crime Scene Integrity

A. Extreme care should be taken to preserve the integrity of any crime scene.

1. Other than to provide necessary first aid and medical care, no one should enter or disturb a suspected crime scene until the appropriate investigator is on site and in control of the scene.
2. Inmates/probationers/parolees and any staff not involved in the security or investigation of the scene should be removed.
3. All potential witnesses should be sequestered until interviewed by appropriate investigators.
4. The scene should be cordoned off and all traffic and onlookers should be kept at an appropriate distance. In an incident such as an escape, care should be taken not to disturb footprints and other signs that may aid a tracking team.

B. Crime scene integrity is particularly important in the event of a death.

1. The room or housing area where a suspected homicide or suicide is discovered must be immediately cordoned off after the body has been examined by the ranking medical staff on duty.
2. No person will be allowed to enter until the appropriate investigator arrives on the scene.
3. If the victim is obviously dead, the body is not to be moved until the investigator approves removal of the body.

C. *The Sexual Assault Victim Search/ Evidence Collection Protocol*, see Operating Procedure 038.3, *Prison Rape Elimination Act (PREA)*, will be followed for all investigations into allegations of sexual abuse to maximize the potential for obtaining usable physical evidence for administrative proceedings and criminal prosecutions in accordance with Operating Procedure 030.4, *Special Investigations Unit*, and Operating Procedure 720.7, *Emergency Medical Equipment and Care*. (§115.21[a, b], §115.221 [a, b])

VI. Disposal of Evidence

A. When all rights to appeal in the matter have been exhausted and it is timely and proper to dispose of evidence, the following procedure will occur:

1. The Court should assume possession and control of any evidence entered during a trial. Possession and control of evidence entered in any Court should be in accordance with the directions of the Court.
2. All monies taken as contraband in a facility must be credited to the Commissary Fund and a record of such credit maintained.
3. For all other items of evidence, excluding controlled substances, the Evidence Manager must get approval for disposal from the Chief of Security. Disposal must be witnessed by the Chief of Security or designee.
4. All requests for disposal of controlled substances should be made through the local Commonwealth's Attorney. Disposal and documentation must be in accordance with instructions of the Commonwealth's Attorney and the appropriate Court.

B. Personal property of an inmate/probationer/parolee may not be disposed of without due process and must be handled in accordance with Operating Procedure 802.1, *Offender Property*. Any usable material, excluding weapons, illegal materials, or sexually explicit materials may be donated to any established charity. A permanent record documenting all such transactions must be maintained.

C. Under no circumstances will an employee of the DOC be allowed to retain possession of any contraband found in a facility.

REFERENCES

Operating Procedure 030.4, *Office of Law Enforcement Services*

Operating Procedure 038.1, *Reporting Serious or Unusual Incidents*

Operating Procedure 038.3, *Prison Rape Elimination Act (PREA)*

Operating Procedure 720.7, *Emergency Medical Equipment and Care*

Operating Procedure 802.1, *Offender Property*

Operating Procedure 910.1, *Probation and Parole Office and Staff Safety and Security*

ATTACHMENTS

None

FORM CITATIONS

Evidence Custody Report 030_F13

Digital Storage File Access 030_F14

Device/Memory Card Seizure 030_F20