Virginia Department of Corrections

Authority, Inspection, and Auditing

Operating Procedure 030.1

Evidence Collection and Preservation

Authority:
Directive 30, *Audits and Investigations*

Effective Date: July 1, 2025

Amended:

Supersedes:
Operating Procedure 030.1, November 1, 2021

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:	Ty Keshae Fowlkes Tucker Security Operations Manager	*Signature Copy on File* Signature	5/23/25 Date
Reviewer:	Rodney Younce Security Operations and Emergency Preparedness Administrator	*Signature Copy on File* Signature	5/23/25 Date
Signatory:	Leslie J. Fleming Deputy Director for Institutions	*Signature Copy on File* Signature	5/27/25 Date
Signatory:	Jermiah Fitz Deputy Director for Community Corrections	*Signature Copy on File* Signature	5/27/25 Date

REVIEW

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

COMPLIANCE

This operating procedure applies to all units operated by the Virginia Department of Corrections (DOC). Practices and procedures must comply with applicable State and Federal laws and regulations, American Correctional Association (ACA) standards, Prison Rape Elimination Act (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.

Evidence Manager - The employee designated by the Facility Unit Head or Chief P&P Officer to oversee the secure storage of evidence for the unit.

Facility Unit Head - The person occupying the highest position in a DOC residential facility, such as an institution, field unit, or Community Corrections Alternative Program.

Information Technology Unit (ITU) - The Department of Corrections (DOC) unit that is the central technology management unit and the clearinghouse for all DOC technology initiatives including but not limited to the management of surplus property management. This unit also coordinates all liaison activities with VITA Science Applications International Corporation, and its suppliers.

Intelligence Analyst - Reviews information and creates reliable intelligence products.

Intelligence Specialist - Staff member assigned to the DOC Special Operations Unit that facilitate the DOC statewide information gathering and intelligence process.

Office of Law Enforcement Services (OLES) - DOC sworn law enforcement employees conducting criminal and administrative investigations.

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 a uniform protocol for the proper collection, documentation, 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 in the Department of Corrections (DOC). (5-ACI-3A-42, 5-ACI-3D-17; 4-ACRS-2C-03; §115.21[a., b], §115.221[a., b])

PROCEDURE

I. Evidence

A. The Facility Unit Head or Chief P&P Officer must provide a secure evidence storage area, such as a safe, to store physical evidence for the unit.

1. The Facility Unit Head or Chief P&P Officer will designate an Evidence Manager to oversee the secure evidence storage area.
2. Only designated employees will be authorized to possess the combination or key and access to the secure evidence storage area.
3. The Evidence Manager must keep a logbook in the secure evidence storage area.
   a. Employees must store all physical evidence in the secured evidence storage area and must document in the secure evidence storage log each time items are placed into or removed from the designated secure evidence storage area.
   b. Any employee who accesses or enters the secure evidence storage area must record:
      i. their name;
      ii. the name and title of all employees accessing the area;
      iii. the date and time of the entering or accessing;
      iv. the reason for accessing the area; and
      v. a brief description of any item placed in or removed from the storage area in the secure evidence storage log.

B. Designated employees will have access to a digital storage folder on the DOC network to store audio and video recordings, and other digital evidence.

C. Principle types of evidence:

1. Contraband seized from an inmate, probationer/parolee, employee, visitor, intern, 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 video recordings.
6. Digital evidence such a computer files or data storage media.
7. Electronic.

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

II. Physical Evidence

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

1. Facility
   a. Any employee who discovers this type of contraband must immediately contact the Shift Commander, who will contact the facility Evidence Manager.
   b. The Facility Unit Head or designee must notify the Office of Law Enforcement Services (OLES) in accordance with Operating Procedure 038.1, *Reporting Serious or Unusual Incidents*, when drugs or weapons are found.
2. P&P Districts
   a. Employees will turn contraband related to a probationer/parolee that may be used as evidence 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*.
   b. If the evidence must be retained in a P&P Office, the employee will document the evidence and place it in the custody of the designated Evidence Manager in accordance with this operating procedure.

B. When physical evidence is discovered, the employee discovering the evidence will document the date, time, and location where the item was discovered. As soon as practicable, this information will be entered on an *Evidence Custody Report* 030_F13.
   1. If an OLES Agent or a local or state law enforcement officer 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 always remain in the possession or control of the discovering employee 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 area.
      a. If the secure evidence storage area 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 employees have access.
      b. The item should be left there until turned over to the Special Operations Unit or OLES, 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 Special Operations Unit or OLES should be held as per this operating procedure and handled as directed by the Special Operations Unit Investigator or OLES Agent.

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 OLES, 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 Storage Folder

A. Only designated employees who were requested and approved by the Facility Unit Head on the *Digital Storage File Access* 030_F14 have access to the facility's digital storage folder.

1. All requests for access must be submitted on the *Digital Storage File Access* 030_F14; requests submitted in any other manner will not be approved.
2. The Facility Unit Head or designee must submit a separate *Digital Storage File Access* 030_F14 to the Regional Administrator for each requested employee.
3. The Regional Administrator must forward the *Digital Storage File Access* 030_F14 to the Security Operations and Emergency Preparedness Administrator for final approval and assignment by Information Technology Unit (ITU) Security.
4. The Regional Administrator must submit a *Digital Storage File Access* 030_F14 for regional employees to the Security Operations and Emergency Preparedness Administrator for final approval and assignment by ITU Security.
5. All other access requests 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.
6. Once assigned to ITU Security an ITU employee or the Security Operations and Emergency Preparedness Administrator will send confirmation with connection details to the employee.

B. The digital storage folder is suitable for securely storing audio and video recordings and other digital documents that may be needed as evidence to include the following:

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

C. Employees must upload audio, video, and digital evidence to the facility's designated digital storage

folder immediately after the incident is concluded and will label the evidence with a specific file name such as WRSP041524_1234567-2. The file names consist of the following:

1. Facility name abbreviation.
2. Incident date.
3. Inmate or probationer/parolee DOC number. The number 9999999 may be used if no inmate or probationer/parolee is identified with the incident.

D. A sequential number for multiple files related to the same inmate or probationer/parolee on the same date. The sequential number may indicate 2 different incidents or 2 different recordings of the same incident.

E. Before erasing the recording from the camera or other data storage device, the employee must confirm the evidence was successfully uploaded to the folder.

F. The level of access an employee has to facility files in the facility's digital storage folder varies based on the employee's operational need.

1. Access Levels
   a. Read Only Access.
   b. Read & Execute Access (View).
   c. Read & Write Access (Copy, Save, Send Files).
   d. Remove Access.
   e. Delete Files Access.
2. ITU employees will remove employee access upon receipt of a *Digital Storage File Access* 030_F14 signed by the Security Operations and Emergency Preparedness Administrator.
3. Requests to delete a file from a digital storage folder must be submitted in writing to the Security Operations and Emergency Preparedness Administrator.
   a. The Security Operations and Emergency Preparedness Administrator will review the request and if approved, will forward the written request to ITU Security as authorization to delete the file.
   b. ITU employees will only delete a file with written approval from the Security Operations and Emergency Preparedness Administrator or above.

G. File Retention and Dissemination

1. Digital evidence must be retained for at least five years after the date of the incident. If a lawsuit is filed or an investigation is in progress, digital evidence must be retained until the investigation or lawsuit is completed.
2. Employees must carefully control and always secure cameras and data storage media to prevent unauthorized access to and misuse of digital evidence.
   a. Employees with the relevant Deputy Director or designee approval, only, may provide copies from a file to law enforcement and other non-DOC agencies.
   b. When an investigation is conducted, employees must make recordings and other digital evidence available to the investigators and the evidence must become part of the investigator's file.
   c. When submitting a related *Disciplinary Offense Report*, *Internal Incident Report*, or *Incident Report*, the employees will list the file name(s) but are prohibited from attaching the recording or other digital evidence to the *Report*.

H. 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.

IV. Cell Phones and Digital Devices

A. When an employee seizes or collects a cell phone or other digital device the employee must consult with

the OLES Point of Contact to determine if OLES involvement is necessary.

1. If OLES involvement is necessary, the OLES Agent will determine if a search warrant is necessary for data extraction.
2. If OLES involvement is not necessary, the employee must mail, or hand deliver the cell phone or digital device to the OLU Intelligence Analyst for data extraction.

B. When a cell phone or digital device is seized or collected from an inmate, probationer/parolee, employee, visitor, or civilian, the employee must:

1. Ask the individual for any charging cords or data cables related to the device.
2. Ask the individual for the passcode. Some passcode protected devices cannot be accessed using available equipment without the passcode.

C. Employees must not attempt to manipulate or view the data on the cell phone or digital device utilizing the passcode.

1. Any viewing or manipulation of the data on the device may require a search warrant.
2. The employee may be required to explain any manipulation or viewing of data later in court.

D. The employee who seized or collected the device must secure the device and any accessories in an evidence bag or envelope.

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

E. The OLES Agent, OLU Intelligence Analyst, or Institutional Investigator, as appropriate, should take charge of the sealed evidence container for secure handling.

1. To request data extraction, the employee should complete a *Device/Memory Card Seizure* 030_F20.
2. The employee must forward the cell phone or digital device, a completed *Device/Memory Card Seizure* 030_F20, and an *Evidence Custody Report* 030_F13 to the appropriate authority. The employee must either:
   a. Give the item to the OLES Agent or the OLU Intelligence Specialist.
   b. Mail the item to Special Operations Unit, Attn: Cell Phone Extraction Request, 3525 Woods Way, State Farm, Va. 23160 via Registered Mail - Return Receipt Requested. The Return Receipt is proof that the cellphone or digital device was delivered for chain of custody purposes.

F. The OLU Intelligence Analyst who extracts the data must forward their findings to the appropriate investigator(s), as needed.

V. Crime Scene Integrity

A. Employees must take extreme care 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 employee not involved in the security or investigation of the scene must 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 employee on duty.
2. No person will be allowed to enter until the investigator arrives on the scene.
3. If the victim is obviously dead, the body is not to be moved until the investigator approves for the body to be removed.

C. Employees must follow *The Sexual Assault Victim Search/ Evidence Collection Protocol* 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, *Office of Law Enforcement Services*, Operating Procedure 038.3, *Prison Rape Elimination Act (PREA)*, 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 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 will 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 receive 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 must 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. Employees must not dispose of inmate and CCAP probationer/parolee Personal property without due process and the disposal must be handled in accordance with Operating Procedure 802.1, *Inmate and CCAP Probationer/Parolee Property*.

1. Any usable material, excluding weapons, illegal materials, or sexually explicit materials may be donated to any established charity.
2. 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, *Inmate and CCAP Probationer/Parolee 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