| | | | |
|---|---|---|---|
| | **Operating Procedure** | **Effective Date** July 1, 2018<br>**Amended** 11/1/18 | **Number** 030.1<br>**Operating Level** Department |
| | | **Supersedes** Operating Procedure 030.1 (6/1/15) | |
| | | **Authority** COV §53.1-10, §53.1-25 | |
| **Subject** **EVIDENCE COLLECTION AND PRESERVATION** | | **ACA/PREA Standards** 4-4207, 4-4233, 4-4282; 4-ACRS-2C-03; §115.21, §115.221 | |
| **Incarcerated Offender Access** Yes ☐ No ☒ | **Public Access** Yes ☒ No ☐<br>**Attachments** Yes ☐ No ☒ | **Office of Primary Responsibility** Director of Security and Correctional Enforcement | |

I. 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.

II. COMPLIANCE

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

III. 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

IV. PROCEDURE

A. Evidence

1. 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. (4-4207, 4-4282; 4-ACRS-2C-03; §115.21[a., b], §115.221[a., b])
2. Each facility and P&P District shall designate an employee to serve as the Evidence Manager to oversee secure storage of evidence for their unit.
3. Each facility and P&P District shall designate a secure evidence storage space for that unit.
   a. 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 shall be documented.
      i. 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.

ii. A logbook shall be kept in each secure evidence storage area. Any person opening the secure evidence storage area shall 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.

b. 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.

4. Principle types of evidence:
   a. Contraband seized from an offender, visitor, staff, or found on DOC property
   b. Hardcopy documents
   c. Reports of chemical or laboratory tests
   d. Forensic physical or trace evidence collected from a victim or crime scene
   e. Audio and/or video recordings
   f. Digital evidence - computer files or data storage media
   g. Electronic
5. Reports related to investigations, incidents, disciplinary actions (staff or offender), or legal action should include a description of any relevant evidence and the disposition of that evidence. (4-4233)

B. Physical Evidence

1. 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.
   a. In facilities, any officer or other employee discovering this type of evidence shall immediately contact the Shift Commander, who shall contact the designated Evidence Manager. The DOC Special Investigations Unit shall be notified in accordance with Operating Procedure 038.1, *Reporting Serious or Unusual Incidents*, when drugs or weapons are found.
   b. In P&P Districts, contraband related to an offender 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 shall be documented and placed in the control of the designated Evidence Manager in accordance with this operating procedure.
2. When an item of physical evidence is discovered, the individual employee discovering the item shall document the date, time, and location the item was discovered. As soon as practicable, this information shall be entered on an *Evidence Custody Report* 030_F13.
   a. If the Special Investigations Unit 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).
   b. The employee who originally discovers the item of evidence should maintain complete control of the item.
   c. The discovering employee shall not pass the item of evidence to another employee for inspection but it shall 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.
3. If the employee discovering the evidence needs to transfer the evidence to another individual, the discovering employee shall 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.
4. All items of evidence should be placed in an evidence container, sealed, and stored in the following manner:
   a. The employee shall 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 shall be wrapped in aluminum foil. *Caution*: Weapons or other items, from which fingerprints may be detected, should not be stored in plastic bags.)

b. 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.

c. All properly sealed evidence containers and *Evidence Custody Reports* shall be given personally to the appropriate Evidence Manager as soon as possible with the transfer documented in the *Chain of Custody* section.

d. 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.

i. 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.

ii. The item should be left there until turned over to the DOC Special Operations Unit or Special Investigations Unit, used in Court, or the case has otherwise been resolved.

e. 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.

f. Evidence related to any investigation conducted by the DOC Special Operations Unit or Special Investigations Unit should be held as per this operating procedure and handled as directed by the DOC Special Operations Unit or Special Investigations Unit Investigator.

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

a. Alcohol discovered within the facility, other than that involved in an investigation, shall be destroyed under supervision of two employees and a record maintained of such destruction.

b. All illegal drugs other than alcohol, or other material involved in an official investigation, shall be turned over to the DOC Special Investigations Unit, local or state police, or, upon a Court order, destroyed in an appropriate manner by facility personnel, and a record of the transaction maintained.

c. 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.

d. 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.

C. Digital Items and Audio/Video Recordings as Evidence

1. 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:

a. Camera recordings and Rapid Eye clips related to incidents

b. Recordings of offender telephone calls

c. Digital photographs of evidence

d. Incoming or outgoing offender secure messages

e. Any other evidence suitable for storage in a digital format

2. Management of Digital Storage Folders

a. Digital evidence shall be given a file name consisting of the facility name abbreviation, date of the incident, offender number, and a sequential number added if there are multiple files related to the same offender on the same date.

i. 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 offender number 1234567 (this may be 2 different incidents or 2 different recordings of the same incident.)

ii. Offender number 9999999 may be used if no offender is identified with the incident.

b. 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.

c. The file name(s) shall be listed in the related *Internal Incident Report*, *Disciplinary Offense Report*, or *Incident Report*. The recording shall not be attached to the *Report*.

3. Digital Storage Folder Access

a. Access to facilities' designated network storage folders is available to authorized users only. Approved users will receive confirmation and connection details from the office of the CTSU Administration and the Director of Security and Correctional Enforcement. All access requests must be submitted on the *Digital Storage File Access* 030_F14; requests submitted in any other manner will not be approved.

b. 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.

c. A separate *Digital Storage File Access* 030_F14 shall be completed for each request for staff access and must be submitted to the Regional Operations Chief, and forwarded to the Director of Security and Correctional Enforcement for final approval and assignment by CTSU staff.

d. Levels of access to files on the facility's digital storage folder will vary depending on operational needs and may include:

i. Read Files Access - i.e., Auditors

ii. Read & Execute Access (View) - i.e., Department Duty Officers, Regional Duty Officers, Special Investigations Unit, others as designated by the Facility Unit Head i.e., Administrative Duty Officers

iii. Read & Write Files Access (Copy, Save, Send Files) – i.e. Institutional Investigator, Intelligence Officer

iv. Delete Files - CTSU staff only with written approval of Director of Security and Correctional Enforcement.

(a) Requests for the deletion of files from a facilities' Digital Storage Folder must be submitted in writing to the Director of Security and Correctional Enforcement.

(b) The Director of Security and Correctional Enforcement will review the request and if approved, the written request will be forwarded to CTSU as authorization to delete the file.

v. Remove Access - CTSU staff only with approval of Director of Security and Correctional Enforcement

e. The Regional Operations Chief will request access for Regional Office staff utilizing the *Digital Storage File Access* 030_F14 submitted to the Director of Security and Correctional Enforcement for final approval and assignment by CTSU staff.

f. All other requests for access must be submitted on the *Digital Storage File Access* 030_F14 to the Director of Security and Correctional Enforcement for approval and assignment by CTSU staff.

g. Copies of files may be provided to law enforcement and other non-DOC agencies only with the approval of the Chief of Corrections Operations or designee.

h. Cameras and data storage media must be carefully controlled and secured at all times to prevent unauthorized access to and misuse of digital evidence.

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

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

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

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

D. Cell Phones

1. 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.
2. If a device is seized or collected from a non-offender, consult with the Special Investigations Unit (SIU) Point of Contact (POC) or Commonwealth's Attorney to determine if a search warrant is necessary for data extraction.
3. A search warrant is not required to seize or extract data from a device in offender possession.
4. Leave device in original state and wrap in aluminum foil immediately.
5. If the device is seized or collected from an individual, ask them for the passcode. Using the equipment available, some passcode protected devices can't be accessed without the passcode.
6. Staff should not attempt to manipulate or view the data on the device by utilizing the passcode unless exigent circumstances exist. Any manipulation of the data on the device may have to be explained later in Court.
7. If the device is seized or collected from an individual, ask them for any charging cords or data cables related to the device.
8. The employee that seized or collected the device shall secure the device and any accessories in an evidence bag or envelope and seal it like any other piece of evidence. Ensure mobile device is wrapped in aluminum foil.
   a. Note the date, time, and location of the seizure for chain of custody purposes.
   b. The appropriate investigator (SIU Agent, Intelligence Specialist/Cellebrite, or Institutional Investigator) should take charge of the sealed evidence container for secure handling.
9. To request data extraction, the appropriate investigator should complete a *Device/Memory Card Seizure* 030_F20.
10. The device and the *Device/Memory Card Seizure* 030_F20 should be given to the SIU Agent, Intelligence Specialist/Cellebrite, 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.
11. The Intelligence Specialist/Cellebrite conducting the data extraction shall complete a *Data Extraction from Electronic/Memory Digital Device Report* 030_F21 and provide findings to the appropriate investigator(s) as needed.

E. Crime Scene Integrity

1. Extreme care should be taken to preserve the integrity of any crime scene.
   a. 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.
   b. Offenders and any staff not involved in the security or investigation of the scene should be removed.
   c. All potential witnesses should be sequestered until interviewed by appropriate investigators.
   d. 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.
2. Crime scene integrity is particularly important in the event of a death.
   a. The room or housing area where a suspected homicide or suicide is discovered shall be immediately cordoned off after the body has been examined by the ranking medical staff on duty.

b. No person shall be allowed to enter until the appropriate investigator arrives on the scene.

c. If the victim is obviously dead, the body is not to be moved until the investigator approves removal of the body.

3. *The Sexual Assault Victim Search/ Evidence Collection Protocol* (see Operating Procedure 038.3, *Prison Rape Elimination Act (PREA)*) shall 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. See Operating Procedure 030.4, *Special Investigations Unit,* and Operating Procedure 720.7, *Emergency Medical Equipment and Care,* for additional guidance. (§115.21[a, b], §115.221 [a, b])

F. Disposal of Evidence

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

a. 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.

b. All monies taken as contraband in a facility shall be credited to the Commissary Fund and a record of such credit maintained.

c. For all other items of evidence, excluding controlled substances, the Evidence Manager shall get approval for disposal from the Chief of Security. Disposal shall be witnessed by the Chief of Security or designee.

d. All requests for disposal of controlled substances should be made through the local Commonwealth's Attorney. Disposal and documentation shall be in accordance with instructions of the Commonwealth's Attorney and the appropriate Court.

2. Personal property of an offender may not be disposed of without due process and shall be handled in accordance with Operating Procedure 802.1, *Offender Property*.

3. 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 shall be maintained.

4. Under no circumstances shall an employee of the Department of Corrections be allowed to retain possession of any contraband found in a facility.

## V. REFERENCES

Operating Procedure 030.4, *Special Investigations Unit*

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*

## VI. FORM CITATIONS

*Evidence Custody Report* 030_F13

*Digital Storage File Access* 030_F14

*Device/Memory Card Seizure* 030_F20

*Data Extraction from Electronic/Memory Digital Device Report* 030_F21

VII. REVIEW DATE

The office of primary responsibility shall review this operating procedure annually and re-write it no later than three years after the effective date.

*Signature Copy on File* *5/9/18*

A. David Robinson, Chief of Corrections Operations Date