# Virginia Department of Corrections

**Technology**

## Operating Procedure 310.1

## *Technology Management*

**Authority:**
Directive 310, *Technology Management*

**Effective Date:** January 1, 2024

**Amended:**

**Supersedes:**
Operating Procedure 310.1, January 1, 2021

**Access:** ☐ Restricted ☒ Public ☐ Inmate

**ACA/PREA Standards:** 5-ACI-1F-04

| | | | |
|---|---|---|---|
| **Content Owner:** | Felicia Stretcher<br>Deputy Chief Information Officer | *Signature Copy on File*<br>Signature | 11/4/2023<br>Date |
| **Reviewer:** | Zacc Allen<br>Chief Information Officer | *Signature Copy on File*<br>Signature | 11/8/2023<br>Date |
| **Signatory:** | Joseph W. Walters<br>Deputy Director for Administration | *Signature Copy on File*<br>Signature | 11/27/2023<br>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

**Accidental** - Theft, loss, vandalism, defacement, or damage that occurred despite staff having used reasonable care in safeguarding Information Technology equipment.

**Agency Information Technology Representative (AITR) -** The Code of Virginia requires that each agency designate an existing staff member to be the agency's information technology representative (AITR) who will be responsible for compliance with the procedures, policies, and guidelines established by the Chief Information Officer of the Commonwealth. The AITR acts as liaison between the DOC and VITA, ensuring that information (issues, concerns, questions etc.) flow smoothly between the two parties and is communicated as needed.

**Business Relationship Manager (BRM) -** The Science Applications International Corporation and its supplier's staff member who manages Information Technology (IT) operations and service delivery for agencies, serves as first customer escalation point for service delivery issues, supports work request solution implementation, assesses performance of IT infrastructure through service level measurement, and reviews results with customers.

**Chief Information Officer (CIO)** - The DOC position responsible for the management of DOC technology resources and for coordinating DOC technology activities with the IT Partnership; prior to the expenditure of DOC funds, all technology initiatives within the DOC will be reviewed and cleared by the CIO. In addition, the CIO is responsible for maintaining and updating the Technology Strategic Plan. The DOC IT Steering Committee will be consulted as needed to provide field input to this process.

**Customer Account Manager (CAM)** - The VITA staff member responsible for establishing and maintaining relationships with customers and managing overall customer satisfaction, serves as second escalation for service delivery and develops understanding of agency business needs to effectively plan for impending changes.

**DOC IT Steering Committee** - A permanent committee whose mission is to identify, evaluate, prioritize applications for implementation that will enhance the operation of the Department of Corrections. The Director, Chief of Corrections Operations, and Deputy Director of Administration and Deputy Director of Programs, Education, and Reentry are members of the IT Steering Committee; Information Technology Unit provides technical and administrative support to the Committee.

**Gross Negligence** - A conscious and voluntary disregard for the need to use reasonable care in safeguarding IT equipment where staff knew or should have known that their actions or failure to act would result in the theft, loss, vandalism, defacement or damage of IT equipment.

**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.

**Inmate Technology –** Includes but is not limited to agency specific hardware and software technologies utilized by inmates/probationers/parolees in all facilities and other organizational units within the DOC.

**IT Partnership (ITP)** - The public-private partnership between the Commonwealth of Virginia and Science Applications International Corporation and its suppliers, which is transforming state government's IT infrastructure technology and providing the expertise and resources to support improved delivery of services.

**Local Support Associate (LSA)** - A LSA will be assigned at every DOC location to provide user support and local coordination with ITU and Science Applications International Corporation and its suppliers staff resources. Web Contacts/Authors should be assigned at any facility/unit that maintains a presence on the DOC intranet.

**Negligence** - Failure to use reasonable care in safeguarding IT equipment where staff actions or failure to act resulted in the theft, loss, vandalism, defacement, or damage of IT equipment.

**Science Applications International Corporation (SAIC) and its Suppliers** - Contract vendor responsible for the service delivery of the Commonwealth's IT infrastructure needs, with oversight from VITA.

**Security Incident** - An IT security event that has an adverse effect on an IT system, service, network, and/or device, or the threat of the occurrence of such an event. The event could be either intentional or accidental in nature and must pose a threat to the integrity, availability, or confidentiality of an IT system.

**Smartphone** – A mobile phone device with advanced capabilities and runs complete operating system software that provides a standardized interface and platform for application developers.

**Software Application Authorizer** - The "owner" of a software application who approves access rights and privileges for a specific application relating to DOC business (e.g., VACORIS, CARS, CIPPS, iDOC, TMS, etc.)

**Wireless Device** - Any smartphone, flip phone, MiFi, or tablet.

## PURPOSE

This operating procedure governs the management of technology resources and responsibilities within the Department of Corrections (DOC). Additionally, it describes the organizational relationship between the DOC and the Information Technology (IT) Partnership as it relates to technology management. The IT Partnership, comprised of the Virginia Information Technologies Agency (VITA) and Science Applications International Corporation (SAIC) and its suppliers, provides information technology services to Virginia's state government.

## PROCEDURE

I. DOC IT Assets (5-ACI-1F-04)

A. Users are responsible for safeguarding any IT assets.

1. DOC IT users are responsible for safeguarding all DOC issued IT assets.
   a. Users are personally accountable for any IT asset they are assigned from the DOC and are responsible for ensuring proper use and security of the asset. DOC issued IT assets must be kept under direct physical control of the user, whenever possible.
   b. When the asset is not under direct physical control of the user, the user must physically secure the assets (i.e., by means of lock and key, in a locked vehicle out of public view, etc.)
   c. Users must not personalize, deface, or otherwise damage DOC issued IT equipment (i.e., laptop, desktop, tablet, cellphone, etc.)
2. The user must immediately report the theft, loss, vandalism, defacement, or damage of any IT asset to the Organizational Unit Head and must submit an incident report for review by the Organizational Unit Head in accordance with Operating Procedure 038.1, *Reporting Serious or Unusual Incidents*.
   a. When IT equipment is stolen, lost, vandalized, or defaced the user must report the incident to the Information Security Officer (ISO) immediately and submit an *ITU Security Incident Report* 310_F6 in accordance with Operating Procedure 310.2, *Information Technology Security*.
   b. When IT equipment is damaged the user must immediately report the incident by email to the ITU at ITRequests@vadoc.virginia.gov, by submitting a ticket to the VCC Helpdesk to determine if the device can be repaired or if the device is damaged beyond repair.
   c. If a wireless device is lost, stolen or damaged, the notification should be sent by email to DOCVoice@vadoc.virginia.gov.
   d. A copy of the incident report and when applicable, the police report must be forwarded electronically to the Agency Information Technology Representative (AITR).
3. The Organizational Unit Head in consultation with the ISO and AITR, as necessary, will be responsible for determining the following:
   a. If an incident was due to an accident, user negligence, user gross negligence, or intentional employee misconduct.
   b. Any cost incurred by the DOC for lost, stolen, or damaged devices to include the cost incurred through the end of the device's refresh term as assed by the IT partnership.
   c. If staff will be required to pay any assessed amount or the cost of repairs to the equipment, the amount paid by staff will be equal to the following:
      i. If it is determined that the first incident is due to negligence, staff will be required to reimburse the DOC 50% of the assessed amount.
      ii. If two or more incidents occur within 12 months due to negligence, staff will be required to reimburse the DOC 100% of the assessed amount.
      iii. If it is determined that the incident is due to gross negligence or intentional staff misconduct, staff will be required to reimburse the DOC one hundred percent of the assessed amount.
4. The Organizational Unit Head, after reviewing all available information, will make a recommendation to the Regional Operations Chief or, as appropriate, the Director, Chief of Corrections Operations, or

a Deputy Director on the following:

a. The cause of the incident, e.g., accident, negligence, gross negligence, or intentional misconduct.

b. The assessed amount to be paid by staff will be managed by the respective business unit and/or region.

c. Any staff disciplinary action under Operating Procedure 135.1, *Standards of Conduct*.

5. The Regional Operations Chief or, as appropriate, the Director, Chief of Corrections Operations, or Deputy Director, will make a final decision on the recommendations and will communicate their decision to the Organizational Unit Head and AITR.

B. Requests for managed network equipment (e.g., desktop, laptop, tablet, printers, etc.) should be forwarded to ITRequests@vadoc.virginia.gov. Appropriate approvals are required from the Information Technology Unit (ITU) Administration & Operations Manager and the Deputy Director for Administration or designee(s) before the equipment is procured.

1. The request for computers should include the staff name in which the device will be assigned, contact information, and tentative start date.

2. Assigned computer equipment is staff specific. Staff maintains the equipment until either it is refreshed or the staff member is no longer employed with the DOC.

C. Requests for telecommunication services (e.g., cellular phones, smartphones, mobile Wi-Fi hotspot devices, analog lines, VoIP, etc.) should be forwarded to DOCVoice@vadoc.virginia.gov. Cellular phones apply to any device issued by the DOC that makes or receives phone calls, leaves messages, sends text messages, accesses the Internet or downloads, and allows for the reading of and responding to email.

D. Appropriate approvals are required for wireless devices from the Regional Operations Chief, Chief Information Officer (CIO), or ITU Administration & Operations Manager and/or the Deputy Director for Administration or the Deputy Director of Programs, Education, and Reentry before the services are procured.

1. All wireless device requests must be made in writing; and should include the staff name to which the device will be assigned, contact information, and a tentative start date.

2. Wireless devices are generally assigned to a specific staff member. Staff will maintain the device until the device is refreshed, no longer required for their position, or they separate from the DOC.

3. When a wireless device is not assigned to a specific staff member but shared among multiple staff in the unit, each staff member using the wireless device must sign Attachment 1, *Wireless Device Acceptable Use Agreement*. The *Wireless Device Acceptable Use Agreement* must be scanned and emailed to DOCVoice@vadoc.virginia.gov.

4. ITU will notify staff receiving the wireless device when the device is ready for pick-up or is shipped to their respective unit.

a. The wireless device will be issued with a battery, wall charger, case, and any operating instructions for staff records.

b. Staff issued the device must sign a *Wireless Device Receipt* 310_F7 and Attachment 1, *Wireless Device Acceptable Use Agreement*, for each DOC issued wireless device to confirm receipt of the device and accessories, and to acknowledge they have read, understand, and agree to adhere to the requirements in the *Wireless Device Acceptable Use Agreement*.

c. The completed and signed *Wireless Device Receipt* and *Acceptable Use Agreement* must be scanned and emailed to DOCVoice@vadoc.virginia.gov within ten business days of receiving the device.

d. Staff who are on short-term disability, long-term disability, military duty, etc., should turn their wireless devices into the unit's business office so that the device can be placed on a billing suspension until they return.

e. Upon separation or reassignment to a new position within the DOC that does not require the wireless device; the device and accessories must be returned immediately to the Organizational Unit Head/designee or the ITU.

f. When iPhones are returned, staff are required to either remove the pin from the iPhone or provide the PIN to DOC Voice. Staff are also required to provide the apple id password. Staff are no longer allowed to wipe the iPhone prior to returning the device.

g. The agency will withhold the value of the COV smart device from staff pay if not returned upon request or termination.

i. With appropriate approval and completion of the *Wireless Device Receipt* 310_F7 and the *Wireless Device Acceptable Use Agreement* by the receiving staff member, the wireless device may be reissued.

ii. If the device is reissued, the completed and signed *Wireless Device Receipt* and *Wireless Device Acceptable Use Agreement* must be scanned and emailed to DOCVoice@vadoc.virginia.gov within ten days business days of receiving the device.

iii. If the device is not reissued, the Organizational Unit Head or designee has ten business days to notify and return the device and accessories to ITU.

iv. All staff who are issued wireless devices or approved for Bring Your Own Device (BYOD) program are required to keep the operating system up to date.

v. All records relating to Commonwealth business are considered to be Commonwealth data, even though generated on BYOD smart device.

vi. State business records are subject to review and disclosure unless the Freedom of Information Act permits or requires them to be withheld.

5. Each organizational unit will have differing requirements for cellular usage, therefore the organizational units are encouraged to standardize models that best fit their operational duties and assist in minimizing support and administration costs.

6. Staff are responsible for proper care and safeguarding of the cell/smart phone.

a. At all times, staff must safeguard the cell/smart phone against loss or theft.

b. Staff assigned cell/smart phones should maintain the phone on their person at all times during duty hours or, if the cell/smart phone is not in use, maintain the cell/smart phone out of sight in a secure (locked) desk drawer or file cabinet.

c. If a staff member is charging the cell/smart phone, the device must not be left unattended without proper safeguards against loss or theft.

d. Unauthorized or inappropriate use of DOC cell/smart phone may result in:

i. Loss of use of said device.

ii. Disciplinary action.

iii. Being held personally liable for any costs associated with the inappropriate use.

7. It is the responsibility of the Organizational Unit Head or designee to ensure that when cell/smart phones and wireless devices that are no longer functional or have been upgraded or replaced, the old device should be returned to ITU within ten business days for proper data destruction and disposal.

a. Approval for disposal should be obtained by emailing DOCVoice@vadoc.virginia.gov.

b. Upon obtaining approval, the equipment should be shipped to the DOC Headquarters - Attn: ITU-Telecommunications Coordinator.

8. Per *Telework Agreement* 110_F4, neither the agency nor the State will be responsible for operating costs, home maintenance, or any other incidental costs (e.g., utilities, internet service providers, long distance phone charges, etc. associated with the use of the staff member's residence, unless pre-approved and detailed in the *Telework Agreement*).

E. DOC staff have the option with appropriate approvals to utilize the BYOD program. The purpose of this program is to provide qualification, authorization, deployment, and use of personal wireless

communication devices for which authorized staff receive a semi-monthly monetary allowance.

F. It is the responsibility of the Organizational Unit Head or designee to ensure that the battery backup Uninterruptable Power Supply (UPS) for the network and Unified Communications as a Service (UCaaS) are sufficiently refreshed to maintain power to the unit infrastructure for no less than five minutes for facilities and 30 minutes for Probation and Parole Offices and Regional Offices.

1. It is also their responsibility to order new batteries when it is determined that the batteries need to be replaced.
2. Specifications and sourcing for the batteries can be obtained by emailing DOCVoice@vadoc.virginia.gov.

G. Requests for IT services or an outage report should be forwarded to VITA Customer Care Center at (866) 637-8482 or email the VCCC at vccc@vita.virginia.gov. Email should not be used to report critical issues or outages impacting operations at any DOC location.

H. Procurement authority - In-scope and out-of-scope

1. Desktop/laptop/tablet hardware - ITU staff will coordinate the procurement of desktop/ laptop/ tablet hardware through the Commonwealth-authorized eVA and work request process documented in the VITA IT Procurement Manual.
2. The desktop/laptop/tablet hardware will be at current Commonwealth standards.
   a. Desktop refreshes will be provided at the five-year refresh cycle.
   b. Laptops at the four-year refresh cycle.
   c. Tablets at the discretion of the DOC.
   d. The hardware will be shipped with the standard DOC image. Hardware break/fix will be provided by SAIC and its suppliers End User Support.
3. The Microsoft Surface tablets are owned by the DOC; therefore, any issues with this hardware should be reported to the VCCC Helpdesk and ITRequests@vadoc.virginia.gov and handled via the manufacturer's warranty.
4. VITA is responsible for the procurement of all IT and telecommunications goods and services on behalf of Executive Branch Agencies and Institutions.
   a. To promote cost savings and administrative efficiency, VITA has delegated some of its procurement authority back to agencies.
   b. This delegation includes the authority to procure specific IT consumables and DOC-specific applications (up to $100,000) without VITA's direct oversight and should not be V-coded.
5. Procurement authority is delegated to DOC by VITA for printers which are not networked or shared and whose purchase price does not exceed $1,000 per order. Therefore, the consumables should be ordered directly, utilizing an "R" code.
6. All network attached printers and multifunction printers are under VITA's authority and should be requested utilizing the VR1 code. Printers have a recurring monthly charge to cover service, support, and network access.
7. The consumables list, network printer and copier options are available on VITA's website IT Goods and Services List.

I. The IT Partnership and ITU IT Operations will collaborate to track and control the inventory of DOC IT assets. Users are responsible for replying to the periodic VITA Asset Validation Survey for their assigned devices and updating information as necessary.

J. Information technology security controls include, but are not limited to, the requirements of all statutes and best practices listed in Commonwealth Security Standard - Sec 501; see Operating Procedure 310.2, *Information Technology Security*.

K. Surplus

1. The organizational units are required to notify ITU of IT surplus via email to ITRequests@vadoc.virginia.gov. In this request, a clear description of the device should be provided to include: the make, model, serial number, and asset tag number, if it exists.
2. Upon receipt of the request, it is the IT Asset Inventory Specialist's responsibility to determine if this equipment is out-of-scope to the IT Partnership (i.e., not supported by SAIC and its suppliers).
   a. If the item in question is deemed in-scope, the request for surplus is denied, and the inquiring unit will be instructed to initiate a ticket with the VCCC.
   b. Once the equipment is determined to be out of scope, the organizational unit will manage the surplus process of the equipment in accordance with Operating Procedure 260.2, *Surplus Property,* or as otherwise instructed by the ITU Administrator and Operations Manager or designee(s).
3. Data on IT assets must be removed prior to disposal in accordance with the *Removal of Commonwealth Data from Electronic Media* Standard (COV ITRM Standard SEC514-03); see Operating Procedure 310.2, *Information Technology Security*.

II. Inmate and Community Corrections Alternative Program (CCAP) Probationer/Parolee Technology

A. Requests for inmate and CCAP probationer/parolee technology services should be sent to the unit's service request ticketing system *School Dude* at www.schooldude.com.

B. Each DOC unit should have at least one person in each department that utilizes inmate and CCAP probationer/parolee technology with a *School Dude* account at www.schooldude.com to submit service requests.

III. DOC-ITP Coordination

A. The CIO, AITR, and IT Partnership, to include the Business Relationship Manager and Customer Account Manager will maintain regular communications and ensure periodic joint key employee meetings to ensure a positive and productive relationship between the DOC, SAIC and its suppliers, and VITA. Additionally, the AITR will ensure the IT Partnership is made aware of DOC technology requirements and any plans for technology initiatives impacting the DOC Network.

B. The IT Partnership will ensure upgrades and modifications that may potentially impact application performance, and any other changes to the network, are communicated to and coordinated with appropriate DOC staff prior to execution whenever practical. Planned shutdowns will be communicated in advance to allow users to prepare.

C. Local Support Associate (LSA) - A LSA will be assigned at every DOC location to provide user support and local coordination with SAIC and its suppliers employee resources. Web Contacts/Authors should be assigned at any unit that maintains a presence on iDOC.

IV. Technology Initiatives

A. The Organizational Unit Head will ensure that any proposed technology initiative is reviewed and cleared by the CIO prior to the expenditure of any DOC funds, or before the start of a software development effort using ITU staff. The CIO will determine whether involvement from the DOC IT Steering Committee is needed.

B. The CIO review of technology initiatives will ensure a thorough assessment of the technology requirements, coordination with ITP, and consideration of the scope of the initiative. The depth and duration of this assessment will depend on the size and complexity of the proposed initiative.

C. Routine procurements for replacement of computers, printers, and other incidental technology assets are not generally considered a technology initiative.

D. All procurements are required to be made in accordance with Operating Procedure 260.1, *Procurement*

*of Goods and Services*.

V. Application Support

A. The ITU is responsible for supporting and maintaining any centrally approved software application, except those maintained under separate contract.

B. Assigned system analysts are responsible for ensuring required coordination with the Software Application Authorizer or the identified "owner" of the application.

C. Development of routine reports, maintenance, and simple enhancements to existing applications is not considered a technology initiative.

VI. Information Technology Security

A. DOC is responsible for establishing IT security requirements in accordance with VITA standards, policies, and guidelines. SAIC and its suppliers is responsible for implementing the DOC requirements across the DOC Network.

B. Operating Procedure 310.2, *Information Technology Security*, governs the DOC IT security requirements.

VII. Virginia Criminal Information Network (VCIN) Information Technology Sanitation

A. Upon notification that a VCIN terminal has been targeted for managed services refresh or hard drive replacement, the respective site is required to notify ITU IT Operations at ITRequests@vadoc.virginia.gov.

B. ITU IT Operations will provide the sites security tape to physically secure the outside case of the terminal, as well as its power supply.

1. Once the device has been secured, it should be shipped to DOC Headquarters to the attention of the IT Operations Analyst for sanitation.
2. Upon receipt, the secured terminal will be sanitized and returned to the IT Partnership.

C. The sanitation process will include overwriting the media at a minimum of three times prior to disposal or redeployed for use by unauthorized individuals.

1. In addition, the sanitation process will zero out the hard drive utilizing Department of Defense approved software. This process will generate a DOD recognized certificate upon completion.
2. The DOC must maintain written documentation of the steps taken to sanitize the media.
3. The DOC will also ensure that the sanitization is witnessed and/or facilitated by authorized staff.

## REFERENCES

Operating Procedure 038.1, *Reporting Serious or Unusual Incidents*

Operating Procedure 135.1, *Standards of Conduct*

Operating Procedure 260.1, *Procurement of Goods and Services*

Operating Procedure 260.2, *Surplus Property*

Operating Procedure 310.2, *Information Technology Security*

VITA IT Procurement Manual

## ATTACHMENTS

Attachment 1, *Wireless Device Acceptable Use Agreement*

## FORM CITATIONS

*Telework Agreement* 110_F4

*ITU Security Incident Report* 310_F6

*Wireless Device Receipt* 310_F7