Operating Procedure

Effective Date November 1, 2017	**Number** 310.1
Amended 9/18/17, 11/15/17, 4/1/19	**Operating Level** Department
Supersedes Operating Procedure 310.1 (6/1/15)	
Authority COV §2.2-2005, §53.1-10, §53.1-25	
Subject TECHNOLOGY MANAGEMENT	**ACA/PREA Standards** None
Incarcerated Offender Access Yes ☐ No ☒	**Public Access** Yes ☒ No ☐ **Attachments** Yes ☒ #1 No ☐
	Office of Primary Responsibility Chief Information Officer

I. PURPOSE

This operating procedure governs the management of technology resources and responsibilities within the Department of Corrections. Additionally, it describes the organizational relationship between the DOC and the 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.

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

Agency Information Technology Representative (AITR) - The Code of Virginia requires that each agency designate an existing employee to be the agency's information technology representative (AITR) who shall 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.

Agency Operations Manager (AOM) - The Science Applications International Corporation (SAIC) and its suppliers employee who manages 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 Technology Committee will be consulted as needed to provide field input to this process.

Customer Account Manager (CAM) - The VITA employee 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 Technology Committee - A permanent committee whose mission is to identify, evaluate, prioritize, and recommend technology innovations and applications for implementation that will enhance the operation of the Department of Corrections. The Director, Chief of Corrections Operations, and Regional Operations Chiefs appoint members of the Technology Committee; Information Technology Unit (ITU) provides technical and administrative support to the Committee.

Information Technology Unit (ITU) - The Department of Corrections 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 coordinates all liaison activities with VITA and relevant contract vendors.

IT Partnership (ITP) - The public-private partnership between the Commonwealth of Virginia and Science Applications International Corporation (SAIC) 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) - All Organizational Unit Heads share general management responsibility for technology issues within their operational areas. A LSA will be assigned at every DOC location to provide user support and local coordination with ITU and Science Applications International Corporation (SAIC) and its suppliers staff resources. Web Contacts/Authors should be assigned at any facility/unit that maintains a presence on iDOC.

Offender Technology - Includes but is not limited to agency specific hardware and software technologies utilized by offenders in all facilities and other organizational units within the DOC.

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, *e*Inventory, TMS, etc.)

IV. PROCEDURE

A. DOC Information Technology (IT) Assets

1. Users are responsible for safeguarding any IT assets.
   a. DOC IT users are responsible for safeguarding any IT asset they remove from the agency, including keeping these assets under their direct physical control whenever possible, and physically securing the assets (i.e., by means of lock and key) when they are not under their direct physical control.
   b. Users shall not personalize or deface Commonwealth of Virginia equipment (i.e. laptop, desktop, tablet, cellphone, etc.)
2. Requests for managed network equipment (i.e. desktop, laptop, tablet, printers, etc.) should be forwarded to the ITRequests@vadoc.virginia.gov mailbox. Appropriate approvals are required from the Information Technology Unit (ITU) Administration & Operations Manager and the Deputy Director for Administration before the equipment is procured.
   a. The request for computers should include the employee's name in which the device will be assigned, contact information, and tentative start date.
   b. Assigned computer equipment is employee specific. The employee maintains the equipment until either it is refreshed or the employee is no longer connected with the DOC.
3. Requests for telecommunication services (i.e. cellular phones, smartphones, mobile Wi-Fi hotspot devices, analog lines, VoIP, etc.) should be forwarded to the DOCVoice@vadoc.virginia.gov mailbox. Cellular phones applies to any device issued by the DOC that makes or receives phone calls, leaves messages, sends text messages, surfs the Internet or downloads, and allows for the reading of and responding to email.
4. Appropriate approvals are required for wireless devices from the Regional Operations Chief, Chief Information Officer, or ITU Administration & Operations Manager and the Deputy Director for Administration before the services are procured.
   a. All wireless device requests must be made in writing; and should include the employee's name to which the device will be assigned, contact information, and a tentative start date.
   b. Wireless devices are generally assigned to a specific employee, the employee will maintain the

device until the device is refreshed, no longer required for the employee's position, or the employee separates from the DOC.

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

d. ITU will notify the employee receiving the wireless device when the device is ready for pick-up or is shipped to their respective unit.
   i. The wireless device will be issued with a battery, wall charger, case, and any operating instructions for the employee's records.
   ii. The employee 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 *Acceptable Use Agreement*.
   iii. The completed and signed *Wireless Device Receipt* and *Acceptable Use Agreement* must be scanned and emailed to the DOCVoice@vadoc.virginia.gov mailbox within ten business days of receiving the device.
   iv. Employees, 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 the employee returns.
   v. 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 Unit Head or their designee, or the ITU.
      (a) With appropriate approval and completion of the *Wireless Device Receipt* 310_F7 and *Wireless Device Acceptable Use Agreement* by the receiving employee, the wireless device may be reissued.
      (b) If the device is reissued, the completed and signed *Wireless Device Receipt* and *Acceptable Use Agreement* must be scanned and emailed to the DOCVoice@vadoc.virginia.gov mailbox within ten days business days of receiving the device.
      (c) If the device is not reissued, the Unit Head or designee has ten business days to notify and return the device and accessories to ITU.

e. 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.

f. Employees are responsible for proper care and safeguarding of the cell/smart phone.
   i. At all times, the employee must safeguard the cell/smart phone against loss or theft.
   ii. Employees assigned cell/smart phones should maintain the phone on their person at all times during duty hours or, if the cell phone is not in use, maintain the cell phone out of sight in a secure (locked) desk drawer or file cabinet.
   iii. If an employee is charging the cell/smart phone, the device shall not be left unattended without proper safeguards against loss or theft.
   iv. Unauthorized or inappropriate use of Agency cell/smart phone may result in
      (a) Loss of use of said device
      (b) Disciplinary action
      (c) Being held personally liable for any costs associated with the inappropriate use

g. 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.
   i. Approval for disposal should be obtained by emailing DOCVoice@vadoc.virginia.gov
   ii. Upon obtaining approval, the equipment should be shipped to the DOC Headquarters - Attn:

ITU - Telecommunications Coordinator.

5. DOC employees have the option with appropriate approvals to utilize the Bring Your Own Device (BYOD) program. The purpose of this program is to provide qualification, authorization, deployment, and use of personal wireless communication devices for which authorized employees receive a semi-monthly monetary allowance.
6. It is the responsibility of the Organizational Unit Head or designee to ensure that the battery backup (UPS - Uninterruptable Power Supply) for the network and UCaaS (Unified Communications as a Service) are sufficiently refreshed to maintain power to the Agency infrastructure for no less than five minutes for Correctional Centers and 30 minutes for Probation Parole Offices and Regional Offices. It is also their responsibility to order new batteries when it is determined that the batteries need to be replaced. Specifications and sourcing for the batteries can be obtained by emailing DOCVoice@vadoc.virginia.gov.
7. Requests for IT services or an outage report should be forwarded to VITA Customer Care Center at (866) 637-8482 or e-mail the VCCC at vccc@vita.virginia.gov. E-mail should not be used to report critical issues or outages impacting operations at any DOC Site.
8. Procurement Authority - In-scope & Out-of-scope
   a. Desktop/Laptop/Tablet hardware - ITU staff coordinates the procurement of desktop/ laptop/ tablet hardware through the Commonwealth-authorized eVA and Work Request process documented in the VITA IT Procurement Manual.
   b. The desktop/laptop/tablet hardware will be at current Commonwealth standards. Desktop refreshes will be provided at the five year refresh cycle, laptops at the four year refresh cycle and tablets at the discretion of the Agency. The hardware will be shipped with the standard DOC Agency image. Hardware break/fix will be provided by Science Applications International Corporation (SAIC) and its suppliers End User Support (EUS).
   c. The MS 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.
   d. VITA is responsible for the procurement of all IT and telecommunications goods and services on behalf of Executive Branch Agencies and Institutions. To promote cost savings and administrative efficiency, VITA has delegated some of its procurement authority back to agencies. This delegation includes the authority to procure specific IT consumables and agency-specific applications (up to $100,000) without VITA's direct oversight and should not be V-coded.
   e. Procurement authority is also delegated to executive branch agencies for printers which are not networked or shared and purchase price does not exceed $1,000 per order. Therefore, the consumables should be ordered directly, utilizing an "R" code.
   f. 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.
   g. The consumables list, network printer and copier options are available on VITA's website IT Goods and Services List.
9. 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.
10. 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*)
11. Surplus

a. The Organizational Units are required to notify ITU of IT surplus via the ITRequests@vadoc.virginia.gov mailbox. 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.

b. 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 Science Applications International Corporation (SAIC) and its suppliers.

i. 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.

ii. Once the equipment is determined to be out of scope, the Organizational Unit shall 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.

c. Data on IT assets shall 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*)

B. Offender Technology

1. Requests for offender technology services should be sent to the agency's service request ticketing system *School Dude* at www.schooldude.com.

2. Each DOC Unit should have at least one person in each department that utilizes offender technology with a *School Dude* account at www.schooldude.com to submit service requests

C. DOC-ITP Coordination

1. The CIO, Agency Information Technology Representative (AITR), and IT Partnership, to include the Agency Operations Manager (AOM) and Customer Account Manager (CAM) will maintain regular communications and ensure periodic joint key staff member meetings to ensure a positive and productive relationship between the DOC, Science Applications International Corporation (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.

2. 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.

3. Local Support Associates (LSAs) will be assigned at every DOC location to provide user support and local coordination with Science Applications International Corporation (SAIC) and its suppliers staff resources. Web Contacts/Authors should be assigned at any unit that maintains a presence on iDOC.

D. Technology Initiatives

1. 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 Technology Committee is needed.

2. 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.

3. Routine procurements for replacement of computers, printers, and other incidental technology assets are not generally considered a technology initiative. All procurements are required to be made in accordance with Operating Procedure 260.1, *Procurement of Goods and Services*.

E. Application Support

1. The ITU is responsible for supporting and maintaining any centrally approved software application, except those maintained under separate contract. Assigned system analysts are responsible for

ensuring required coordination with the Software Application Authorizer or the identified "owner" of the application.

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

F. Information Technology Security

1. DOC is responsible for establishing IT security requirements in accordance with VITA standards, policies, and guidelines. Science Applications International Corporation (SAIC) and its suppliers is responsible for implementing the DOC requirements across the DOC Network.

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

G. VCIN Information Technology Sanitation

1. Upon notification that a Virginia Criminal Information Network (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. ITU IT Operations will provide the sites security tape to physically secure the outside case of the terminal, as well as its power supply. Once the device has been secured, it should be shipped to DOC Headquarters to the attention of the IT Operations Analyst for sanitation. Upon receipt, the secured terminal will be sanitized and returned to the IT Partnership.

2. The sanitation process will include overwriting the media at a minimum of three times prior to disposal or redeployed for use by unauthorized individuals. The sanitation process will zero out the hard drive utilizing DOD approved software. This process will generate a DOD recognized certificate upon completion. The agency shall maintain written documentation of the steps taken to sanitize the media. The agency shall also ensure that the sanitization is witnessed and/or facilitated by authorized personnel.

V. REFERENCES

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

VI. FORM CITATIONS

Wireless Device Receipt 310_F7,

VII. REVIEW DATE

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

The office of primary responsibility reviewed this operating procedure in November 2018 and necessary changes have been made.

Signature Copy on File *9/13/17*

N. H. Scott, Deputy Director for Administration Date