| | | |
|---|---|---|
| | **Technology** | |
| | **Operating Procedure 310.2** | |
| | *Information Technology Security* | |
| | **Authority:**<br>Directive 310, *Technology Management* | |
| | **Effective Date:** February 1, 2023 | |
| | **Amended:** 3/1/23, 5/1/23, 2/1/24, 4/1/24 | |
| | **Supersedes:**<br>Operating Procedure 310.2, July 1, 2022 | |
| | **Access:** ☐ Restricted  ☒ Public  ☐ Inmate | |

# Virginia Department of Corrections

**ACA/PREA Standards:** 5-ACI-1F-01, 5-ACI-1F-03, 5-ACI-1F-06, 5-ACI-1F-07, 5-ACI-1F-08; 4-ACRS-7D-05, 4-ACRS-7D-06; 4-APPFS-3D-31, 4-APPFS-3D-34; 2-CO-1F-01, 2-CO-1F-06; 2-CI-2C-1, 2-CI-2C-2

| | | | | |
|---|---|---|---|---|
| **Content Owner:** | Atron Thorne<br>Information Security Officer | *Signature Copy on File* | | 1/11/2023 |
| | | Signature | | Date |
| **Reviewer:** | Zacc Allen<br>Chief Information Officer | *Signature Copy on File* | | 1/11/2023 |
| | | Signature | | Date |
| **Signatory:** | Joseph W. Walters<br>Deputy Director for Administration | *Signature Copy on File* | | 1/17/2023 |
| | | Signature | | 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 January 2024 and necessary changes are being drafted.*

*The content owner reviewed this operating procedure in January 2025 and necessary changes are being drafted.*

## 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

**Criminal Justice Information Services (CJIS) -** The Federal Bureau of Investigations (FBI) division responsible for the collection, warehousing, and dissemination of relevant criminal justice information to the FBI, law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

**Data** - Raw, unorganized facts (written or electronic) that are in the possession of Department of Corrections employees, volunteers, vendors, or contractors.

**Data Sharing** - An agreement between the DOC and another federal, state, or local government agency, where the agency is granted access to DOC systems and can export DOC data as approved in the agreement.

**Information** - Processed, organized, or structured data related to employees, inmates/probationers/parolees, incidents or operational units, to include: writings of all kinds, email, correspondence, memoranda, notes, diaries, statistics, receipts, letters, returns, summaries, pamphlets, books, interoffice and intra-office communications, bulletins, printed matter, computer printouts, system logs, database logs, word processing files, calendars, scheduling programs, teletypes, facsimiles, drawing, sketches, spreadsheets, oral records, photographs, video, tape recordings, magnetic discs, and any other recordings.

**Information Technology (IT)** – Equipment, interconnected system, or subsystem used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.  This term includes computers, peripherals, software, firmware, similar procedures, services, and related resources.

**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.

**Intern** - An individual who is undergoing supervised practical training and is serving an internship to advance their area of study, without compensation from the DOC.  Interns receiving compensation from the DOC are considered employees and will be managed in accordance with their employment status. (updated 2/1/24)

**Internet** - A global collection of interconnected computer networks sharing a wide variety of resources (research and archived data, publications, news, weather, electronic mail, etc.) and functionality including "e-government", communications, and entertainment.  No one individual is in charge of, or owns, the Internet.  Internet Service Providers (ISP s) offer the vehicle for access to the Internet.  Internet Service Providers (ISPs) offer the vehicle for access to the Internet.

**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.

**ITU Security** - The information security section within the ITU; the Information Security Officer (ISO) is the head of ITU Security.

**Local Site Support** (**LSS**) - An individual whose primary responsibilities are not related to IT, but provides IT support to others within the same operating unit (e.g., VACORIS).

**Malware** *("malicious software")* - Programs or files designed to infiltrate and damage a computer system without the owner's knowledge.  Malware includes computer viruses, worms, Trojan horses, rootkits, spyware, some adware, malicious, and unwanted software.  (Also, see Virus, Worm)

**Non-DOC Requests** - Software application requests by government agencies (Federal, State, Local) that have a valid need to access DOC software applications (e.g., VACORIS).

**Obscene Material** - Any material that "considered as a whole, has as its dominant theme or purpose an appeal to the prurient interest in sex, that is, a shameful or morbid interest in nudity, sexual conduct, sexual excitement, excretory functions or products thereof or sadomasochistic abuse, and which goes substantially beyond customary limits of candor in description or representation of such matters and which, taken as a whole, does not have serious literary, artistic, political or scientific value." (COV §18.2-372, *Definition of Obscene*)

**Organizational Unit Head** - The person occupying the highest position in a DOC organizational unit, such as a correctional facility, Regional Office, Probation and Parole Office, Virginia Correctional Enterprises, Academy for Staff Development, Infrastructure and Environmental Management Unit, Agribusiness Unit, and individual Headquarters units, e.g., Human Resources, Offender Management, Internal Audit.

**PC** - Personal computer, which also applies to all DOC workstations, including laptop computers.

**Political Activity** - An activity involving or relating to individual views about social relationships involving authority or power (political opinions); involving or relating to the profession of governing (political office); having or influenced by partisan interests (political party).

**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.  (updated 2/1/24)

**Sensitive Information** - Data that must be protected from unauthorized access or disclosure to safeguard the privacy and security of an individual or organization.  Sensitive information can be on paper, electronic (computer or phone), or verbal.

**Smart Device** - An electronic device capable of connecting to a network, or to other devices, via wireless communication protocols, and which can operate interactively and autonomously to some extent. It includes devices that exhibit some properties of ubiquitous computing, such as artificial intelligence.

**Social Media** - Form of online communication or publication that allows for multi-directional interaction. Social media includes blogs, wikis, podcasts, social networks, photograph and video hosting websites and new technologies as they emerge. Examples of social media outlets include, but are not limited to, Facebook, Instagram, LinkedIn, Reddit, TikTok, Tumblr, Twitter, WhatsApp and YouTube, etc.

**Software Applications** - Software used by DOC employees to perform needed job duties (e.g., VACORIS, CARS, FAACS, Inmate Pay/Inmate Trust, etc.).

**Software Applications 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.).

**System Administrator** - Analyst, engineer, or consultant responsible for implementing, managing, or operating a DOC IT system at the direction of the System Owner, Data Owner, and/or Data Custodian.  The System Administrator manages day-to-day administration and implements security controls and other requirements of DOC IT systems.

**System Owner** - Manager responsible for operation, maintenance, and documentation of risk for a DOC IT system.

**User ID** - The name given to a user or account that enables access to the computer system/network.

**Virginia Information Technologies Agency (VITA)** - The agency responsible for the central management of the Commonwealth's information technology resources.

**Virus** - A program that can replicate itself and infect a computer without the user's knowledge.  The difference between a virus and a worm is that a virus requires a host program in order to replicate.  A virus can only spread from one computer to another when its host is taken to an uninfected computer and spread to other computers by means of a network file system, USB, CD, etc., then accessed by other computers.  For a virus to replicate, it must be permitted to execute code and write to memory.  This is the reason; many viruses attach themselves to executable files, which are part of legitimate programs. (Also, see Malware, Worm)

**Volunteer** - Any citizen of the community who, of their own free will, provides goods or services to the DOC without any financial gain.

**Wireless IT Equipment -** Equipment, including 802.11 a/b/g and Bluetooth or any equipment connecting to or interacting with DOC information technology systems without the use of wires such as: wireless access points, wireless cards, cellular cards or phones used to access other networks while connected to the DOC's network,

handheld PCs and personal information managers utilizing Bluetooth or 802.11 a/b/g to access any network while still connected to the DOC network.

**Workstation** - The device used by employees to connect to the network or system resources.  Workstation also means personal computers and laptop computers.

**Worm** - A self-replicating computer program, which uses the computer network to send copies of itself to other computers attached to the network, without any user intervention.  Unlike a virus, a worm does not need to attach itself to an existing program, meaning it can spread itself to other computers without needing to be transferred as part of a host.  A worm does its damage by spreading through the network exploiting vulnerabilities in operating systems and almost always causing harm to the network.  *(Also, see Malware, Virus)*

# PURPOSE

This operating procedure establishes security controls in accordance with Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Information Security Standard COV ITRM Standard SEC501 and standards for the acceptable use of the Internet, email, and electronic communications tools. Virginia state law requires the Agency Director to become, and remain, compliant with all COV ITRM security requirements as noted in Code of Virginia §2.2-603 (F), *Authority of agency directors*.

# PROCEDURE

I.    Organizational Responsibilities

A. Applicability

1. COV ITRM Standard SEC501 and COV ITRM Standard SEC525 defines the security requirements to protect DOC data and information from loss, unauthorized use, modification, disclosure, or reproduction, and to ensure the implementation of, and compliance with, controls, standards, and procedures.

2. This operating procedure implements COV ITRM Standard SEC501 and COV ITRM Standard SEC525 to govern the security of DOC information and data collection system, including verification, access to data, and protection of the privacy of inmates/probationers/parolees and employees. (2-CO-1F-06)  It ensures that all data and information, and the means by which they are created, gathered, processed, transmitted, communicated, and retained are identified, classified, controlled, and safeguarded. (2-CI-2C-1)

3. DOC data and information must also meet federal, state, and other regulatory and legislative requirements, including the Federal Bureau of Investigations Criminal Justice Information Services policies and procedures and Virginia State Police's Virginia Crime Information Network policies and procedures.

4. This operating procedure applies to all DOC employees, contractors, volunteers, interns, and partners requiring access to or the use of DOC Information Technology (IT) Resources. (2-CI-2C-2)

5. Employee failure to follow this operating procedure is a violation of Operating Procedure 135.1, *Standards of Conduct*, and may result in disciplinary action.

B. Information Technology Unit (ITU) Organizational Structure

1. The Chief Information Officer (CIO) of the ITU is responsible for DOC IT resources.

2. The CIO must approve all DOC software applications development and acquisitions to be used by multiple users.  There are no exceptions.  Applications created, procured, or installed without this approval will not be supported by ITU, are still required to meet all VITA/COV security standards, and may be required to be uninstalled.

3. The Deputy Chief Information Officer of the ITU is responsible for DOC IT resources as delegated by the CIO or in the absences of the CIO.

4. The Information Security Officer (ISO) is responsible for IT Security and will implement and maintain the DOC information security program.

a. The ISO will ensure that adequate and appropriate levels of protection are established to ensure data remains confidential, accurate with integrity, and both the system and data will remain available.  The ISO will ensure that adequate technical resources are in place to prevent unauthorized or unnecessary access or disclosure, and ensure effective and accurate processing and continuity of operations as relates to IT security within the DOC.

b. The ISO will create, implement, enforce, and maintain security policies, procedures, and IT security programs for DOC IT resources and systems under the direction of the Agency Director and in conjunction with the CIO.

c. The ISO may appeal through the chain of command to the Deputy Director for Administration for

review and resolution of a security issue.

    d.  The ISO will maintain liaison with the Chief ISO of the Commonwealth.

5.  The Agency Information Technology Resource (AITR) provides oversight of operational technology activities to include routing, switching, and telecommunications in support of institutions and community corrections as well as the maintenance of IT asset inventory and software licenses. Administration functions include billing, procurement, transfer, and disposal of assets.

6.  The AITR is responsible for ensuring cooperative sharing of information between the agency and Virginia Information Technologies Agency (VITA).

C.  The Application Development Manager and the IT Delivery Services Manager work together to address all custom application development, project management, software acquisitions, database administration, and ensuring adherence to security standards, guidelines, and procedures.

1.  The IT Partnership (VITA/SAIC) will configure and deploy all DOC servers and workstations not identified by the ISO as being related to security. Servers and workstations will be configured in accordance with the VITA/SAIC server and workstation standard configuration procedures. ISO designated security servers are supported solely by the ISO and other security employees. VITA/SAIC is responsible for all contracted hardware maintenance.

2.  Organizational Unit Heads will ensure that policies and procedures relative to IT security are enforced in accordance with this operating procedure.

3.  In order to complete the annual IT Security Awareness Training requirements, all salaried and wage employees, consultants, volunteers, interns, and authorized users having a DOC IT system account are required to read and consent to the terms of the *DOC Information Security Agreement,* see *Windows User Information Security Agreement* 310_F3.

4.  VITA/SAIC is designated and responsible for creating DOC network account access and subsequent activities (additions, deletions, transfers, renames, disk quota allocations, etc.).

    a.  VITA/SAIC is responsible for monitoring all DOC network accounts for adherence to the COV ITRM Security Standard SEC 501 and SEC 525. VITA/SAIC is therefore responsible for compliance, with their scope of duties, to all other related relevant codes, laws, and policies applicable to DOC IT.

    b.  DOC relies on VITA/SAIC IT operations for management of DOC network accounts. DOC cannot perform oversight on VITA/SAIC IT operations' management of DOC network accounts.

II.    Access to DOC IT Resources

A.  Requests for account maintenance and activities must be communicated to the DOC ITU Security Office.

1.  Accounts must be granted on the basis of least privilege. The principle of least privilege requires that access is only provided to the systems that are required of the user to complete their functions; see Operating Procedure 310.4, *External Users Access Control*. DOC system account access must be documented following VITA/COV security standards. Users are encouraged to utilize the *DOC System Application Request* 310_F10, if current procedures are not compliant with VITA/COV security standards.

2.  COV network account access requests are managed as follows, in accordance with VITA/COV security standards:

    a.  All new user account requests must include a *Windows User Account Request* 310_F2 submitted to ITU Security.

    b.  Each request for a new account must include a *Windows User Information Security Agreement* 310_F3 signed by the user. This must be kept in the user's employee file locally.

    c.  All user re-name account requests must include a *Windows User Account Request* 310_F2 submitted to ITU Security.

    d.  All requests for account transfers must be submitted by the receiving location utilizing a *Windows*

*User Account Request* 310_F2 to ITU Security, within 24 hours of the transfer.

    e. All requests for account disables must include a *Windows User Account Request* 310_F2 submitted to ITU Security.

    f. Any user going on a leave of absence expected to last 30 days or more must have their account disabled for the duration of their absence.

    g. For an account to be re-enabled, the user's Supervisor, Human Resources Officer (HRO), Organizational Unit Head, or ITU Security must include a *Windows User Account Request* 310_F2 submitted to ITU Security.

    h. VITA requires in the Security Standards (SEC 501 and SEC 525) to retain accounts in a disabled state, for a time-period compliant with Library of Virginia data retention requirements.

    i. In accordance with VITA Security Standards, a request to disable an account must be submitted to ITU Security within 24 hours of the separation or termination of any employee or contractor.

3. Guest and shared accounts are prohibited on sensitive systems.

4. All DOC employees requiring Admin/System Accounts must submit a *Windows Admin/System Account Request* 310_F4 to ITU Security. A signed copy of the *Windows Admin/System Security Agreement* 310_F1 will be sent to ITU Security. Each System Administrator must have a resource backup for the purposes of business continuity.

5. Requests for access to shared folders must be submitted to ITU Security, defining the specific access required. For example: the name of the shared folder and the type of access needed. To be written similar to: \\s3groups\James River\Dairy Modify or Read only access.

6. Access to a facility's designated digital storage folder will be assigned through ITU Security in accordance with Operating Procedure 030.1, *Evidence Collection and Preservation*.

7. Requests for access to another user's information (mail or shared folders) must be submitted to ITU Security.

8. As authorized by the Organizational Unit Head, interns may be granted Windows User Accounts and VACORIS access with the following requirements:

    a. To access VACORIS, interns must have completed the same background process as employees; see Operating Procedure 102.3, *Background Investigation Program*.

    b. Security Awareness Training, Gang Training, and other procedural requirements must be followed as for employees.

    c. Interns should have similar access as their respective DOC counterpart i.e., Counselors, P&P Officers, etc.

    d. For employees working at one DOC organizational unit (facility, for example) and interning at another DOC organizational unit (P&P Office, for example), both Organizational Unit Heads must approve the additional job functions.

    e. The Organizational Unit Head is responsible to terminate access to DOC IT systems immediately at the end of the internship.

9. Volunteers are prohibited from access to DOC IT systems and VACORIS unless authorized by the Regional Operations Chief (Chief of Corrections Operations or Deputy Director for volunteers not serving in a facility or P&P Office).

    a. Once access is properly authorized, background, training, and access requirements are the same as interns above.

    b. The Organizational Unit Head is responsible to terminate access to DOC IT systems immediately at the end of the volunteer's need for access.

B. Accounts must be validated periodically to determine if the access is still necessary

1. VITA/SAIC and ITU Security will monitor account usage. Accounts that have not been logged into after 90 days will be disabled. After 120 days of inactivity, accounts may be deleted upon request of

the business unit contact.

2.  VITA/SAIC must also conduct a review of all Domain Admin, Server Admin, and System accounts. Accounts not being utilized within 90 days will be deleted. This will ensure compliance with all local, state, and federal requirements, including Criminal Justice Information Services.

3.  For disciplinary suspensions greater than one day, accounts and physical access must be disabled.

C.  Remote Access (CISCO AnyConnect + RSA Dual Authentication Token/Global Protect/Prisma)

1.  Remote access via the IT Partnership enterprise solution (AnyConnect/Global Protect/Prisma) is provided to all users and is installed on all devices.

2.  Access

    a.  The Organizational Unit Head will need to submit an email to ITU Security to request new users be granted access to AnyConnect/Global Protect/Prisma and provided a token for authentication for AnyConnect.

    b.  Dual Authentication (RSA Token) will be assigned to the user by ITU Security.

    c.  When a hard token is issued and the token is lost or damaged, ITU Security must be notified immediately.

3.  Use of any remote connection to DOC IT Systems constitutes acceptance of and agreement to this operating procedure. Remote connections to DOC IT Systems may be monitored, scanned, or analyzed at any time without notification or consent.

4.  All remote connections to DOC IT Systems must originate from a DOC owned device excluding authorized contractors with approved equipment.

5.  All systems connected to the DOC IT Systems remotely must be running virus protection with current virus definitions.

6.  All systems connected remotely to the DOC IT Systems must be up to date on all current operating system and software security hotfixes, service packs, patches, and updates.

7.  Users not in compliance with this operating procedure and its conditions will not connect to DOC IT Systems.

8.  All systems connected remotely to the DOC IT Systems must utilize a firewall to protect the DOC from any other systems originating the remote connection.

D.  Non-DOC Requests for Access to DOC IT Systems

1.  All requests for data sharing must be approved by the Data Governance Board.

2.  This type of access is provided utilizing the IT Partnership enterprise solution Secure Web Access Portal (SWAP).

    a.  All initial requests by non-DOC users for access to DOC software applications or systems must be submitted in writing to the CIO or to ITU Security. The requestor must submit clear justification for the need for access to the DOC Systems. Once approved by the CIO or ITU Security, ITU Security will notify the requestor when access is granted. The request must include the following information:

        i.  The type of access required

        ii.  Direction of dataflow

        iii.  Contact information for the organization owning the IT system and/or data, including the System Owner and System Administrator.

        iv.  There must be a written agreement delineating the security requirements for each interconnected IT system and each type of data shared. All future connectivity must be established in the written agreement before implementation can occur.

        v.  The written agreement will also include data handling, storage, and disclosure.

3.  The non-DOC requestor is responsible for notifying ITU Security of removal of access privileges when

access is no longer needed.  Failure to comply with this requirement may result in denial of future requests.

4. The non-DOC requestor will be provided a copy of this operating procedure.  Use of granted access constitutes acceptance and agreement to abide by this operating procedure.

5. Non-DOC entities that are granted Domain Administrator Access must sign the *Windows Admin/System Security Agreement* 310_F1; see Operating Procedure 310.4, *External Users, Access Control*.

E. Software Application Authorization and Revocation

1. Acceptable access to DOC software applications and non-DOC software applications are contingent upon approval by the requestor's Supervisor and the Software Applications Authorizer.

2. All requests for access to DOC software applications (VACORIS, TMS, etc.) or non-DOC software applications (CARS, CAIS, VCIN, etc.) must be sent to and approved by the Software Applications Authorizer listed on Attachment 1, *DOC Applications Access Authorization.* (5-ACI-1F-01, 5-ACI-1F-06, 5-ACI-1F-08; 4-ACRS-7D-05, 4-ACRS-7D-06; 4-APPFS-3D-31, 4-APPFS-3D-34)

   a. It is the responsibility of the Software Applications Authorizer to notify ITU Security of authorized designee additions and deletions.

   b. Questions concerning the authorization list should be directed to the ITU Security mailbox: (ctsusecurity@vadoc.virginia.gov).

3. ITU Security will accept the following valid application authorization requests from the Software Applications Authorizers' and their designees:

   a. Email from the Software Applications Authorizer or their designee.

   b. Written correspondence with a valid authorization signature from the Software Applications Authorizer or their designee.

4. ITU Security will accept the following requests for revocation of privileges:

   a. Email or written correspondence from the DOC managing Supervisor.

   b. The only exception is a request from the DOC Special Investigations Unit or DOC management, due to an investigation or urgent need.  All such urgent requests must be provided by written authorized correspondence for documentation purposes.

5. ITU Security will remove all software application access for account deletions and determine if software application access removal is necessary for account transfers.

6. All software application privileges granted, modified, and/or revoked must be performed by the ITU Security group or their designee.

III.    Usage of DOC IT Resources

A. Network –Authorized Login Accounts

1. User and account access to DOC systems/network must be identified in accordance with *COV IT Information Security Standard* (SEC 501 and/or SEC 525), or by other means providing equal or greater security (e.g., biometric readers, retina scanners etc.), and must be approved by the VITA/SAIC and ITU Security groups before accessing any systems/network resources.

2. Server system software will execute with its inherent account as designed by the manufacturer of the software.

B. Official Use

1. No user will have an expectation of privacy when using DOC IT Systems.

   a. The DOC has the right to monitor all aspects of DOC IT Systems, and such monitoring may occur at any time, without notice and without the user's permission.

   b. Monitoring of IT systems and data may include but is not limited to network traffic, application

and data access, keystrokes, user commands, email and Internet usage, and message and data content.

c. Except for exemptions under the Act, electronic records may be subject to the Freedom of Information Act (FOIA) and therefore, available for public distribution.

d. DOC IT assets/devices must remain in the continental United States at all times, unless explicit prior approval has been granted by the ISO to travel with the assets/devices.

2. ITU Security will monitor use of all DOC Information Systems for any activity that may be in violation of state and/or DOC policy and procedure. ITU Security will review all security settings, configurations, and patch management for security and violations of policy and procedure.

3. The DOC uniformly collects, records, organizes, and processes data, much of which is sensitive and confidential, about employees, inmates/probationers/parolees, and agency operations for management information purposes in order to carry out DOC's Mission, Vision, Goals, and Objectives. (2-CO-1F-01)

4. DOC related business must remain on DOC computers. Do not forward, auto-forward, or direct other staff to forward DOC related business/emails to non-DOC accounts. Personal use of the computer and the Internet - means use that is not job-related. In general, incidental and occasional personal use of the Commonwealth's electronic communications tools, including the Internet is permitted during work hours, but not to interfere with the performance of the employee's duties or the accomplishment of the unit's responsibilities. Personal use is prohibited if it:

a. Adversely affects the efficient operation of the computer system; or

b. Violates any provision of this operating procedure, any supplemental procedure adopted by the agency supplying the Internet or electronic communication systems, or any other policy, regulation, law, or guideline as set forth by Federal, State or Local, law, see COV §2.2-2827, *Restrictions on state employee access to information infrastructure*.

5. Users of the DOC computer system/network must not use these resources for soliciting business, selling products, or commercial activities other than those expressly permitted by DOC management.

6. The Organizational Unit Head will ensure employees, contractors, volunteers, interns, and authorized users will not allow inmates/probationers/parolees to have access (supervised or unsupervised) to any DOC IT resource connected to the agency's network/systems, or resource that can access the Internet. Any exception must be unequivocally approved by the CIO and Deputy Director.

a. Inmates/Probationers/Parolees are strictly prohibited from any access to DOC IT resources on the agency's network/systems or resources that can access the Internet. IT resources not on the agency's network/system or resources that do not have Internet access may be utilized by inmates/probationers/parolees in accordance with Operating Procedure 310.3, *Offender Access to Information Technology*.

b. An exception is provided for supervised inmates in the work release program at Virginia Correctional Enterprises (VCE) with explicit approval of the Deputy Director for Administration.

c. Inmates/Probationers/Parolees will not have direct, unsupervised access to output and storage peripherals such as printers, scanners, DVD burners, and copy machines unless to perform specific educational or job tasks.

d. Inmates/Probationers/Parolees must be under constant sight supervision of DOC employees when performing such tasks. At a workstation in a controlled area with locked doors (such as VCE shops or CTE classrooms) inmate/probationer/parolee use of IT equipment is allowed under the general supervision of a trained employee.

e. DOC employees will inspect printed or copied items to guard against misuse of DOC resources.

f. Any exception to this configuration must be approved by the Chief of Corrections Operations.

7. No access will be granted to any DOC IT System, resource, or data by anyone unless that access is granted in accordance with this operating procedure. Based on the scope of work to be performed, a background check is required.

8. Vendors, partners, or other non-DOC entities will not be granted access to the DOC IT Systems without the express written permission of the CIO.

    a. All requests for data sharing must be approved by the Data Governance Board.

    b. When access is requested, ITU Security will provide the CIO with a risk assessment.

    c. If access is granted by the CIO to a vendor, partner, or non-DOC entity, that entity must agree in writing to abide by all applicable laws, regulations, and DOC operating procedures prior to receiving access; see Attachment 3, *IT Systems Interoperability Security.*

9. Posting sensitive information on a public website, File Transfer Protocol (FTP) server, bulletin board, shared drive, or other publicly accessible medium is prohibited unless a written exception is approved by the DOC Director. The exception must include the business case, risks, mitigating controls, and all residual risks.

10. Certain activities are prohibited when using the Internet, electronic communications, and IT Systems. These include, but are not limited to:

    a. Accessing, downloading, printing or storing information with sexually explicit content as prohibited by law; see COV §2.2-2827, *Restrictions on state employee access to information infrastructure*.

    b. Downloading or transmitting fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images.

    c. Installing or downloading computer software, programs, or executable files in violation of this and other applicable operating procedures.

    d. Uploading or downloading copyrighted materials or proprietary agency information in violation of this and other applicable operating procedures.

    e. Uploading or downloading access-restricted agency information in violation of this and other applicable operating procedures.

    f. Using another employee's DOC network account for any purpose.

    g. Posting information or sending email using another's identity, an assumed name, or anonymously.

    h. Forwarding of joke email, chain letters, personal photographs, etc..

    i. Conducting DOC business with a personally owned external email address (e.g., Gmail, Yahoo).

    j. DOC email addresses will only be used for DOC business, and not to be used as one's own personal email address (i.e., logging in to another company or business websites, signing up for personal items, shopping, or paying bills).

    k. Picture avatars on Gmail/Outlook must contain only a facial photograph that is of a professional nature and deemed business appropriate or an agency or department logo.

    l. The use of language, words, or pictures that could be considered offensive to others.

    m. Permitting a non-user to use DOC resources for purposes of communicating the message of some third-party individual or organization.

    n. Tampering with security controls configured on COV workstations.

    o. Installing or using proprietary encryption hardware or software on COV systems.

    p. Installing personal software on a COV system.

    q. Adding system hardware to, removing system hardware from or modifying system hardware on a COV system.

    r. Connecting non-COV devices to a COV IT system or network, such as personal computers, laptop, PDA or other handheld devices, USB (flash) drives, cell phones, and digital music players.

    s. Utilizing a DOC issued laptop/smart device and/or DOC issued mobile phone as one's own personally owned device for personal business.

    t. Using proprietary agency information, state data records and social media to locate agency customers for personal reasons.

u. Posting photos, videos, or audio recordings taken in the work environment without written consent. This includes photographing/recording DOC material on display screens, monitors, etc.

v. Using agency or organization logos without written consent.

w. Texting, emailing, or using hand-held electronic devices while operating a state vehicle in violation of the *Office of Fleet Management Services Policies and Procedures Manual.*

x. Streaming audio and video, as it not only slows down the network speed but it also clogs network traffic.

y. Providing application data to individuals who do not otherwise have authorization or access to such information.

z. Unacceptable, inappropriate, or unauthorized access, use, disclosure, alteration, manipulation, destruction or misuse of DOC data or information.

aa. Any other activities designated as prohibited by the DOC.

C. Password Security

1. All DOC password requirements are based on the minimum VITA Standards.

2. All users of DOC IT systems must be identified with a non-generic User ID and password or by other means that provide equal or greater security. All non-standard methods of access (e.g., biometric readers, retinal scanners, etc.) must be approved by VITA and ITU Security before accessing any systems/network resources.

3. Employees must not share accounts or allow others access through their User ID unless approved by ITU as a shared account.

4. All accounts must have a password.

5. Passwords must not be displayed on the screen as they are entered.

6. VITA/SAIC will implement and maintain the Windows password policy on the Windows Systems once it has been set by ITU Security.

7. Passwords must be implemented on mobile devices issued by DOC (iPhone, iPad, etc.) The password requirement for mobile devices is a minimum of four characters.

8. All users must choose passwords structured in the following manner:

a. For non-web-based systems where only a login and password are used (dual factor/multifactor *is not* in place), the password must be changed every 42 days, may not be reused for 24 generations, and the following complexity must be met:

Password Length: 14 characters

Must contain three of the four below:
  i. Alpha characters (a-z)
  ii. Numeric characters (0-9)
  iii. Capitalized characters (A-Z)
  iv. Symbols and punctuations (#!$%^&*)

b. For non-web-based systems where a login, password, and a dual factor/multifactor *is* in place, the password must be changed every 60 days, may not be used for 24 generations, and the following complexity must be met:

Password Length: Eight characters

Must contain three of the four below:
  i. Alpha characters (a-z)
  ii. Numeric characters (0-9)
  iii. Capitalized characters (A-Z)
  iv. Symbols and punctuations (#!$%^&*)

c. For web-based where only a login and password are used (dual factor/multifactor *is **not*** in place), the password must be changed every 42 days, may not be reused for 24 generations, and the following complexity must be met:

Password Length: 14 characters

Must contain four of the four below:
   i. Alpha characters (a-z)
   ii. Numeric characters (0-9)
   iii. Capitalized characters (A-Z)
   iv. Symbols and punctuations (#!$%^&*)

d. For web-based systems where a login, password, and a dual factor/multifactor *is* in place, the password must be changed every 60 days, may not be used for 24 generations, and the following complexity must be met:

Password Length: Eight characters

Must contain three of the four below:
   i. Alpha characters (a-z)
   ii. Numeric characters (0-9)
   iii. Capitalized characters (A-Z)
   iv. Symbols and punctuations (#!$%^&*)

e. Examples of how to pick a strong password without making it too complex to remember
   i. Take two words like "two sticks" and capitalize some letters and substitute symbols and numbers.
   ii. Two sticks = Tw0$t1cK$ This password has alpha characters, numeric characters, and punctuation or symbols so it meets the requirements.

   *Note: Do not use this example as your password; this is only an example.*

9. The password must not be related to the user's job or personal life or a word found in the dictionary as most common words can be easily 'cracked' by a password cracking tool.

10. After four unsuccessful attempts to enter a password, the User ID involved will be:
   a. Temporarily disabled
   b. Once a password is locked out, users must contact the VCCC to have the password unlocked

11. Anyone that installs any device or software on DOC systems must change all default passwords on all devices, service accounts, or software before it is used by DOC employees. This refers to all vendor default passwords on all devices or software packages. Passwords must not appear as plain text in any scripts.

12. Passwords must not be written down or left in a place where unauthorized persons might discover them, e.g., under keyboard, top drawer of desk, under mouse pad, taped to PC.

13. If any user suspects that their password may have been disclosed, they must immediately change the password, notify the ISO, or notify ITU Security.

D. Logging off, locking, and rebooting workstations

1. All workstations, when unattended even for short periods must be locked and password protected. The locking screen saver on all PCs has been set to take effect within 30 minutes if there is no activity on the workstation. Devices with access to sensitive systems or those devices in less physically secure environments must have a lower time-out interval documented and enforced, in accordance with *COV ITRM Standard SEC 501 and/or COV ITRM Standard SEC 525*.

2. When users have completed work for the day, they will put their workstation in stand-by mode. Shared workstations must either log off or reboot their workstations. Due to the need to patch software, update virus definitions, or perform other maintenance on PCs after hours, a complete shutdown is not

required unless ITU requests it.

3. All servers must be configured with the screen saver settings to take effect within two minutes and lock the server if there is no activity on the server.

4. Users will reboot their PCs at least weekly to ensure PC health and that security patches and updates that have been applied take effect.

E. Internet Services Usage

1. DOC Internet Sites and Visitor Privacy

   a. The DOC uses VIPNet to host state web sites. To function properly, some VIPNet applications create "cookies" containing information found on users' computers. The applications place those "cookies" on the computers and notify users of their creation.

   b. The DOC Public Internet site does not:
      i. Record personal information of visitors
      ii. Record movements of visitors through the site
      iii. Record dates and times of visits
      iv. Record Internet browser information

   c. DOC reserves the right to modify Internet privacy policy and procedures at any time and without prior notice.

2. Filtering, monitoring, and inspection

   a. The ITU Security Office filters, monitors, and inspects activities and information related to the use of DOC Systems and Internet services to ensure these services are used only for acceptable, appropriate, and authorized purposes. ITU Security blocks access to known pornographic, gambling, and other unacceptable, inappropriate, and unauthorized websites.

   b. An employee is notified of any attempted visit to an inappropriate and unauthorized website, whether intentional or not, by a warning message. The employee will notify their supervisor if they receive a warning message.

   c. An employee must notify their supervisor and ITU Security via the ITU Security Mailbox: ctsusecurity@vadoc.virginia.gov, if they gain access to a pornographic, gambling or other web site designated by the DOC as inappropriate and unauthorized, whether intentional or not.

   d. Unacceptable, inappropriate, and unauthorized use of Internet services, electronic communications, IT Systems, and devices will be investigated and acted on in accordance with Operating Procedure 135.1, *Standards of Conduct*.

   e. If an employee has visited or attempted to visit one or more unauthorized websites the following procedure will be followed:
      i. ITU Security will deliver a written report of the employee's activity to the employee's Organizational Unit Head.
      ii. ITU Security will deliver copies of the report to Human Resources, the Special Investigations Unit, and the CIO.
      iii. The Organizational Unit Head will give notice of the report to the employee, the employee's Supervisor, and to the Organizational Unit Head's Supervisor (i.e., Chief of Corrections Operations, Deputy Director for Administration, Deputy Director for Programs, Education, and Re-entry, Regional Operations Chief, or Regional Administrator).
      iv. The Organizational Unit Head may request the employee's access to the Internet be suspended. Access may be reinstated only if requested by the Organizational Unit Head.
      v. If a supervisor reasonably suspects that an employee has intentionally visited or attempted to visit one or more unauthorized websites, the Supervisor, through the Organizational Unit Head, will request ITU Security to analyze the Internet activity of the employee.

3. Acceptable, appropriate, and authorized usage

   a. DOC Internet services support job functions, communications, information exchange, and

collaborative work.

b. All COV and DOC policies and procedures regarding conduct of employees relevant to the use of Internet services apply to the use of those services.

c. DOC authorizes only legal and ethical use of Internet services.

d. DOC requires users of Internet services to respect copyrights, software licensing rules, property rights, and the privacy and prerogatives of others.

e. Utilization of USB (flash) drives must only include those that are encrypted, unless the use of an unencrypted drive is approved in writing by the Director, Chief of Corrections Operations, or Deputy Directors.

    i. When approved, the unencrypted drive will only be used on a stand-alone, free-standing device. Under no circumstances will an unencrypted drive be connected to or used on any device connected to the DOC network.

    ii. Facility employees must ensure that the drive is removed from the facility upon completion of the approved activity or purpose.

f. Use of Internet services is a privilege that can be revoked.

g. Specific acceptable, appropriate, and authorized usages of Internet services include, but are not limited to, activities supporting:

    i. Job functions, communications, information exchange, and collaborative work directly related to the charter, mission, goals, and purposes of the DOC

    ii. Applications for, and administration of, grants and contracts for DOC research projects or other programs

    iii. Dissemination or distribution of laws, policies, procedures, rules, programs, services, activities, or other official information

    iv. Administrative communications not requiring a high level of security

    v. Employees' pursuit or maintenance of training, education, or certifications related to their job function and responsibilities

    vi. Professional society activities related to employees' job responsibilities and activities

    vii. Administrative communications and discussions related to employees' job responsibilities and activities

h. If a business need requires access to blocked content, access may be requested by the user's Organizational Unit Head via the ITU Security Mailbox: ctsusecurity@vadoc.virginia.gov.

4. Unacceptable, inappropriate, and unauthorized usage

a. DOC has no tolerance for employees, contractors, interns, and volunteers who use DOC Internet services and IT (personal computers, smart devices, networks, etc.) for unacceptable, inappropriate, and unauthorized purposes.

b. If the DOC determines that an employee, contractor, intern, or volunteer has visited or attempted to visit one or more pornographic, gambling, or other web sites designated by the DOC as unacceptable, inappropriate and unauthorized, the employee, contractor, intern, or volunteer must be reported to their Organizational Unit Head for appropriate action under Operating Procedure 135.1, *Standards of Conduct*.

c. Specific unacceptable, inappropriate, and unauthorized usages of Internet services include, but are not limited to:

    i. Violations of federal or state laws or violations of state or DOC policies or procedures

    ii. For-profit activities, excluding those directly related to the DOC's charter, mission, goals and purposes, or employees' job responsibilities and activities

    iii. Private business, including commercial advertising

    iv. Personal or other non-DOC related fund raising or public relations activities, excluding those approved by the Director or the Director's designee

    v. Intentional modification of passwords, files, or other data belonging to another employee

without prior approval from either the employee or their supervisor

vi.   Creation, transmission, retrieval, or storage of material or messages of a libelous, defamatory, derogatory, inflammatory, discriminatory, or harassing nature, including, but not limited to, those relating to race, ethnicity, national origin, religion, political affiliation, sex, gender, and age, or physical, mental, and emotional disability

vii.  Access, use or distribution of computer games that are unrelated to the DOC's mission, goals and purposes, or employees' job responsibilities and activities, but excluding computer games that teach, simulate, or illustrate DOC-related information and activities which are approved by management and then installed by a Local Site Support.

viii. Interference with IT users, services, or equipment including, but not limited to, those usages developing or propagating malicious code, attempting unauthorized access to another employee's computer, distributing advertisements, or sending chain mail

ix.   Using the network to gain unauthorized entry to another machine on the network

x.    Storing of music files or personal photographs on the DOC network Local Authorized Network (LAN)

xi.   Utilizing a personally owned external account (e.g., Gmail, Yahoo) to conduct official DOC business

xii.  Allowing access to the Internet, DOC network, LAN, WAN or other network to any person who has not received access approval from the DOC

xiii. Placing obscene material on the DOC computer network, for use, access, or distribution of sexually explicit, indecent, or obscene material

5.  Pornography

   a.  The use of DOC Internet services or any DOC IT System for visiting pornographic websites, or for accessing, storing, or distributing pornographic material, is prohibited.

   b.  ITU will monitor DOC employees', contractors', interns', and volunteers' Internet access for hits and blocks on pornographic, gambling, and other inappropriate websites. ITU Security will report violations of this operating procedure to the violator's Organizational Unit Head.

   c.  The following laws, standards, and guidelines govern the use of COV and DOC IT, including Internet services, with respect to pornographic websites and materials, and other unacceptable, inappropriate, and unauthorized web sites and materials, by Commonwealth and DOC employees, contractors, interns, and volunteers. Users of DOC Systems must adhere to these procedures, codes, and laws while using DOC Systems.

      i.   Operating Procedure 135.1, *Standards of Conduct.*

      ii.  <u>COV</u> §18.2-374, states, in part, that possession, production, reproduction, publication, distribution, transportation, or sale of obscene items is unlawful.

      iii. <u>COV</u> §18.2-372, *Definition of Obscene*.

      iv.  18 <u>United States Code</u> §1465 states, in part, that interstate transportation or communication, via computer or other means, of obscene materials is unlawful. Any person found in violation of this code will be fined or imprisoned, or both.

      v.   <u>COV</u> §2.2-2827, defines restrictions on state employees' access to any information infrastructure. DOC must immediately furnish current employees with copies of this code section's provisions, and will furnish all new employees copies of this section concurrently authorizing them to use agency computers.

      vi.  <u>COV</u> §18.2-374.1:1, defines possession of child pornography and describes the legal penalty for such acts. All sexually explicit visual material which utilizes or has as a subject a person less than 18 years of age will be subject to lawful seizure and forfeiture pursuant to §19.2-386.31.

F.  Email usage

   1.  The DOC email system and all email accounts and their associated messages and attached files, are the property of the COV and must be used for appropriate business purposes. DOC related business

needs must remain on DOC computers.  Do not forward, auto-forward, or direct other staff to forward DOC related business/emails to non-DOC accounts.

    a. Appropriate use refers to job functions, job communications, information exchange and collaborative work directly related to the mission, goals and business of the DOC.

    b. Personal, non-work related or inappropriate comments, graphics, quotes, links, or other non-business-related items are not permitted in official communications using email or other media.

2. Employees who are members of DOC affiliated associations are permitted to use the DOC email system for association purposes to communicate and share information with other members because it is in the best interest of the DOC to support the development and ongoing education of employees.

    a. Employees are prohibited from using the DOC email system, facilities, equipment, supplies, and work time to lobby for or against a political activity or political candidate on behalf of the association.

    b. Employee use of the DOC email system for association purposes must comply with applicable DOC operating procedures governing the use of state equipment and the requirements of this operating procedure.

    c. Employees who fail to comply with this operating procedure are subject to revocation of this privilege and are subject to disciplinary action in accordance with Operating Procedure 135.1, *Standards of Conduct*.

3. Back-up copies of email messages and attached files may be stored and referenced for operational and legal purposes.  Contents of email messages and files may be disclosed without employees' permission to appropriate and authorized DOC employees and to law enforcement officials.

4. The DOC email systems, and all email accounts and their associated messages and attached files are subject to monitoring by ITU Security to ensure adherence to all relevant DOC policies and procedures, Virginia codes and laws, and United States codes and laws.  This monitoring can occur at any time without the user's consent or notification.

5. Email must not be used to send sensitive information unless encryption is used.  The transmission of email and attached data that is sensitive relative to confidentiality or integrity is required to be encrypted; however digital signatures may be utilized for data that is sensitive relative to integrity.

6. Email at DOC is subject to all the terms and conditions in the *Internet Services Usage* Section of this operating procedure.

7. Any user of the DOC network who receives an email message violating the *Internet Services Usage* requirements will report the incident to their immediate supervisor.  The Supervisor will then contact ITU Security.

8. Posting information or sending electronic communications such as email using another's identity is prohibited.

9. DOC email must not be forwarded to an external email address unless there is a documented business case provided to ITU Security by the Organizational Unit Head.

10. Emails may often be used in legal or other administrative proceedings that were not anticipated when the message was sent.

    a. FOIA requests, court subpoenas, or other unexpected situations can place an electronic message in front of someone that you did not anticipate.

    b. An electronic message is just as "official" as a letter typed on letterhead stationery and mailed to the recipient through the postal service.

    c. Personal or inappropriate comments, graphics, quotes, links, or other non-business related items cannot be included in official communications, electronic or otherwise.

11. Standard framework for electronic message "auto signatures"

    a. Users are required to give their name, office or state cell phone number, and email address when

creating messages and replying to others.  Other information such as job title, agency, and address are encouraged.  For example:

John Doe, Bureau Chief
Virginia Department of Corrections
P.O. Box 26963
6900 Atmore Drive
Richmond, Virginia 23261-6963
Telephone 804-674-3000
Fax 804-674-3001
Email John.Doe@vadoc.virginia.gov

b. At the discretion of the Organizational Unit Head a brief Organizational Unit statement or graphic may be included in employee "auto signatures".

i. The statement or graphic must reflect the DOC Mission, Vision, Healing Environment Initiative, Dialogue and/or Strategic Plan.

ii. The Organizational Unit Head must submit the Organizational Unit's statement or graphic for review and approval to the appropriate Regional Operations Chief for facilities and P&P Offices.

iii. Headquarters units will submit their statement or graphic to the Chief of Corrections Operations, Deputy Director for Administration or Deputy Director for Programs, Education, and Re-entry as applicable for review and approval.

iv. Users may choose to include the standard statement or graphic developed for the Organizational Unit; no other graphics, quotes, links, etc. are allowed in "auto signature".  This does not include a simple graphic or personal comment used in a clearly personal message sent to a single user.

G. Requesting an investigation

1. Only the following designated roles are authorized to request an investigation into an individual's use of DOC IT resources.

a. Agency Head/Director

b. Chief of Corrections Operations; on behalf of the Director or for employees in their chain of supervision

c. Deputy Director for Administration; on behalf of the Director or for employees in their chain of supervision

d. Deputy Director for Programs, Education, and Re-entry; on behalf of the Director or for employees in their chain of supervision

e. Director of Security & Correctional Enforcement, Corrections Operations Administrator, Corrections Administration Manager, or other executive level employee designated by the Director, Chief of Corrections Operations, or appropriate Deputy Director to request an investigation on their behalf

f. Special Investigations Unit Head or Designee

g. Internal Audit Unit Head or Designee

h. Attorney General's Office employees assigned to represent the DOC

i. Administrative Compliance Manager/Legal Compliance Manager

j. Regional Administrator; employees in their respective region, only

k. Regional Operations Chief; employees in their respective region, only

l. Organizational Unit Head; employees in their respective Organizational Unit, only

m. Human Resource Director or Designee (i.e. EEO Manager)

2. All requests for an investigation will be documented electronically on an *Electronic Investigation Request* 310_F8.  All investigation requests will be securely stored for a period of three years.

a. The *Electronic Investigation Request* 310_F8 will include key metrics and parameters for

investigating an employee's use of technology resources.

    b. Highly confidential *Electronic Investigation Requests* e.g., investigation of an Organizational Unit Head will be directed to the Chief of Corrections Operations, Deputy Director of Administration, Deputy Director for Programs, Education, and Re-entry, or the respective Regional Operations Chief, as appropriate.

    c. Only those items documented on the *Electronic Investigation Request* 310_F8, will be searched for or retrieved. The *Electronic Investigation Request* 310_F8, will be amended to include any subsequent requests for auditing purposes.

H. Virus, malware, phishing, ransomware suppression, and remediation

1. All DOC employees are required to exercise caution when opening files/clicking links retrieved from the Internet or received via electronic mail.

2. Files that have been downloaded or received should be subject to the virus checking software provided by DOC before those files are opened or executed.

3. VITA/SAIC is responsible for supporting and maintaining the agency's anti-virus enterprise software and ensuring that current definitions and updates are pushed out to the network/system.

4. Each user will be responsible for contacting ITU Security to provide assistance in correcting any damage to a PC/workstation if it becomes infected with a virus.

5. All PCs/workstations in use within DOC must have VITA/SAIC approved and supported virus suppression software, with the latest release, loaded and activated on their PC/workstation.

6. DOC users are prohibited from intentionally developing, deploying, using, or experimenting with malicious programs, including but not limited to viruses, adware, worms, spyware, Trojans, and keystroke loggers.

7. When a user has introduced malware, phishing, virus, or ransomware onto a DOC device, the following remedial action must occur:

    a. The user must notify their Unit Head when the user believes they are a victim of malware, phishing, virus, or ransomware. The DOC user must also contact ctsusecurity@vadoc.virginia.gov.

    b. The user must complete corrective action retraining through the ITU Security training platform, within 30 days. After the first 21 days, the user's manager will be notified that training has not been completed.

    c. The Unit Head must monitor the user's completion of correction action training and confirm via email to ctsusecurity@vadoc.virginia.gov that training is completed.

I. Security incident reporting (5-ACI-1F-03)

1. An IT security incident refers to an adverse event in an information system, network, and/or workstation, or the threat of the occurrence of such an event.

    a. IT security incidents must be immediately reported to the ISO by emailing ctsusecurity@vadoc.virginia.gov.

    b. If email is known or suspected to be compromised, report the incident through alternate channels that have not been compromised.

    c. In addition, the incident must be reported by telephone to the ISO or CIO.

2. The user will document and report details that may be of relevance including date, time, name(s), location(s), systems, networks, and other significant information. To preserve evidence, no action beyond immediate notification to ITU Security will be taken by any individual without the express direction of the ITU Security Office.

3. All IT security incidents must be reported to ITU Security using the *ITU Security Incident Report* 310_F6. All report information must be emailed to the ITU Security Office (ctsusecurity@vadoc.virginia.gov).

4.  The ISO must report applicable IT Security incidents to the Virginia State Police Fusion Center within 24 hours of receiving notification.

5.  The following are examples of IT security incidents:

    a.  System impairment due to improper usage/denial of service

    b.  Unauthorized access or repeated attempts at unauthorized access from either internal or external sources

    c.  Virus attacks which adversely affect servers or workstations

    d.  Theft, loss, or vandalism of DOC software, hardware, or DOC system devices (including desktops, laptops, tablets, and mobile devices/mobile phones)

    e.  Web site defacement

    f.  Intrusion or intrusion attempts into unauthorized system or user accounts

    g.  Unauthorized access, use, disclosure, alteration, manipulation, destruction, or other misuse of DOC data

    h.  Circumvention of IT security controls, safeguards, or procedures

    i.  Inappropriate use of the Internet or electronic email as defined in this operating procedure

    j.  Connecting to or tampering with another user's PC without written authorization

    k.  Installing hardware or software that has not been approved by ITU

    l.  Accessing or attempting to access, copy, read, or manipulate data in any way that is not owned by the person attempting access, directly related to their job description, or for which the person attempting access has no legitimate right or need to access the information

    m.  Unauthorized release of unencrypted sensitive information (data breach) that is not otherwise obtainable from publicly available resources, or from federal, state, or local government records lawfully made available to the general public.  This information includes first name (or initial) and last name in combination with and linked to any one or more of the following data elements *that relate to a resident of the Commonwealth*, when the data elements are neither encrypted nor redacted:

        i.  Social security number (at least five digits);

        ii.  Driver's license number or state identification number (at least four digits); or

        iii.  Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts

        iv.  Passport number

        v.  Military identification number

        vi.  Any information regarding an individual's medical information.  Medical information is defined as:

            (a) The first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted.

            (b) Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional; or

            (c) An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

6.  If after ITU Security investigates the reported security incident and determines that the incident needs further investigation, ITU Security will notify the Special Investigations Unit to perform a more thorough investigation of the incident.

J.  Criminal History Information, Procedure, and Responsibilities

1.  Criminal history information requested by someone other than the authorized Virginia Criminal

Information Network (VCIN) operator will be personally presented to the requester or sent in a sealed envelope marked "CONFIDENTIAL".

2. A criminal history record must not be given to non-criminal justice agencies and must not be disseminated by radio or telephone except in an urgent or emergency situation, or for purposes of employee safety.

3. A record of all criminal history requests will be maintained in a *Criminal History Request Log* as specified in the VCIN manual.

4. When criminal history records have served the purpose for which they are intended, they must be destroyed by burning or shredding.

5. There will be no unauthorized access or dissemination of any information obtained from VCIN. Violations will be handled in accordance with the COV and Operating Procedure 135.1, *Standards of Conduct.*

K. Telephone usage

1. Personal calls

   a. Local personal calls, which have to be made during working hours may be made from DOC telephones, but their number and duration will be kept to a minimum.

   b. Long distance personal calls must not be made from DOC telephones unless charges are reversed or charged to the employee's personal telephone number or personal credit card account.

2. Employees must not access 900 numbers or any other number for personal use that constitutes a charge to the Commonwealth.

3. Organizational Unit Heads will be responsible for monitoring usage of DOC telephones and reviewing any billing statements to detect inappropriate usage.

L. Storage of photographs

1. Inmate/Probationer/Parolee photographs and photographs of employee or inmate/probationer/parolee special events and activities including but not limited to volunteer banquets, celebrations, ceremonies, etc. may be temporarily stored on the DOC network.

   a. Inmate/Probationer/Parolee photographs taken during visitation will be stored on the network for a maximum period of six months.

   b. Inmate/Probationer/Parolee photographs taken as a part of a facilities picture project and photographs of employee or inmate/probationer/parolee special events and activities may be stored on the network for a maximum period of 90 days.

   c. Photographs that are still needed after the authorized time period has elapsed must be removed from the DOC network and saved to an offline storage device such as a flash drive, CD/DVD or other portable storage device authorized by this operating procedure.

2. Inmate/Probationer/Parolee photographs that are uploaded in VACORIS must not be stored on the network.

3. Photographs used as evidence are subject to the requirements of Operating Procedure 030.1, *Evidence Collection and Preservation*.  Access to a facility's designated digital storage folder will be assigned through ITU Security.

4. ITU Security will monitor the storage of photographs on the network and may remove unauthorized content with notification to the Organizational Unit.

   a. Each month, employees will review their W Drive and DOC email account and remove any items no longer needed.

   b. ITU Security performs routine scans on all drives and will notify the Organizational Unit Head of any employee that has documents or photographs that should not be stored on the DOC network.

IV.   IT System Management

A. Software authorization

1. Special technical software and hardware specifications for special units within DOC will be maintained with those unit's inventories and auditing documentation. No IT Initiative will commence without prior written notification and approval of the CIO of ITU.

   a. The CIO will make appropriate ITU employee assignments (if needed) within two weeks of receipt of the request.

   b. No software for use by more than one user will be bought, downloaded, developed, programmed, or installed on the DOC network without express written approval from the CIO.

      i. The CIO must approve software use that falls outside of the DOC standard configuration. A written request to the CIO must be sent through the requesting employee's Supervisor.

      ii. Requests for software to be installed must be submitted to ITU Security. If not obvious, an explanation of the use for the software is required. Proof of license is also required.

2. Sensitive information will not be used or stored in non-production environments (i.e., a development or test environment must have security controls equivalent to the production environment).

3. VITA/SAIC and ITU Security reserve the right to refuse all software that it considers to be Malware or hacking tools. Any request that is accepted or rejected will be forwarded to ITU Security (ctsusecurity@vadoc.virginia.gov) for follow up with the requestor.

4. DOC is a member of the Microsoft Select and Enterprise Agreement. Membership in this agreement allows DOC to acquire Microsoft Licensing for operating systems and office automation products. Procedures located on DOCNET will be followed when users wish to obtain, procure, and use the products. A hard copy of this operating procedure may be requested through email to the ITU Fiscal Administration and Security group.

5. Employees and contractors must not allow inmates/probationers/parolees access (supervised or unsupervised) to software applications that are not stand-alone; see Operating Procedure 310.3, *Offender Access to Information Technology*.

   a. Facility workstations accessible by inmates/probationers/parolees must be located in offices or enclosed areas that can be locked and secured.

   b. Inmates/Probationers/Parolees must not have direct, unsupervised access to output and storage peripherals such as printers, scanners, DVD burners, and copy machines unless to perform specific educational or job tasks.

   c. Inmates/Probationers/Parolees must be under constant sight supervision of DOC employees when performing such tasks. At a workstation in a controlled area with locked doors (such as VCE shops or CTE classrooms) inmate/probationer/parolee use of IT equipment is allowed under the general supervision of a trained employee.

   d. DOC employees will inspect printed or copied items to guard against misuse of DOC resources.

   e. Any exception must be unequivocally approved by the CIO and Chief of Corrections Operations.

6. All standalone workstations that have been formerly used by inmates/probationers/parolees must be reformatted and their operating systems and software reinstalled by contacting ITU Security prior to attaching the workstation on the DOC network.

7. Users who have to access both their PC and inmate/probationer/parolee standalone workstations must write-protect any data storage media exchanged between networked and inmate/probationer/parolee used machines to avoid infestation of their media with possible viruses or malware.

8. All files on floppy disks, CD's, flash drives, and tapes must be scanned with antivirus software prior to writing data to their PC or network if they have been used on inmate/probationer/parolee PCs or have been used outside of the DOC.

9. The installation of software products that the software publisher has designated as end-of-life (i.e., the

software publisher no longer provides security patches for the product) is prohibited.

10. Employees and contractors must not allow unauthorized individuals access to DOC equipment or DOC software applications used for official purposes.

11. VITA/SAIC is responsible for all security patches, hot fixes, and updates for software on DOC IT Systems. Unless otherwise authorized, users are not permitted to download and apply updates to any software.

12. DOC users are encouraged to save data to their W drive (network share) rather than their computer hard drive (C:\) due to the fact that computers could potentially crash or become infected and a user may lose data. VITA/SAIC does not back up data or systems that are not saved to non-networked locations ("Desktop", "Documents", "Downloads", or "C:\" locations).

B. Hardware authorization

1. No IT hardware will be installed, used on, or connected to DOC IT Systems by non-ITU employees without prior knowledge or approval from VITA/SAIC and ITU Security. Examples include but are not limited to routers, switches, hubs, servers, workstations, wireless IT equipment, PDAs, removable drives and storage, printers, or any other IT device or peripheral.

2. Requests for hardware to be connected to the network must be sent to the VCCC.

3. New and replacement DOC workstations/PCs are leased from VITA. Current specifications and prices can be obtained from the VITA website. Workstations that require reloading or configuring will be returned to the approved image when purchased or otherwise noted by VITA/SAIC.

4. Only DOC approved mobile data storage devices may be used on, or connected to DOC IT Systems. USB devices (e.g., flash drives) utilized within DOC must be encrypted.

5. Vendors, contractors, or any other non-DOC employees who need to connect IT hardware to the DOC Systems must have written approval of ITU Security and be provided a copy of this operating procedure. Any IT hardware attached to DOC IT Systems will be subject to this operating procedure.

6. All hardware systems connected to the DOC Network must utilize appropriate virus protection software and maintain up-to-date virus definitions and will be subject to security scans and will have no expectation of privacy.

7. All IT hardware connected to DOC IT Systems will be up to date with all applicable hot fixes and or security patches.

8. Any vendors, contractors, or non-DOC employees that do not meet this requirement or do not agree to this operating procedure will not connect any devices to the DOC Systems or Network.

9. Donated technology (i.e., computers, software, peripherals etc.) may not be accepted, installed or used by DOC employees and inmates/probationers/parolees without prior written approval by the Chief Technology Officer or Deputy Director for Administration.

C. Wireless Equipment Security

1. Wireless IT equipment has unique security risks and must not be employed within DOC without the written consent of ITU Security, ITU Operations, and the VITA/SAIC teams. Requests for wireless equipment must be sent to either DOC Voice or IT Requests, depending on the nature of the request.

2. Any wireless IT equipment deployed within DOC will be evaluated on a case-by-case basis and may have different requirements based on its requested location and use. CISCO is the standardized wireless equipment utilized within the DOC.

3. Wireless IT equipment is subject to monitoring and scanning by ITU Security at any time without notification or consent and is subject to all aspects of the *Internet Services Usage* and *Hardware Authorization* sections of this operating procedure.

4. All wireless equipment attached to COV DOC IT systems must run 128 bit or greater encryption and be able to successfully pass a wireless security scan by ITU Security.

5. DOC workstations may be connected to trusted wireless networks, which are those networks utilizing a secure encryption protocol such as Wi-Fi Protected Access (Wired Equivalent Privacy is not considered secure), and those managed by another COV agency. DOC workstations may not be connected to untrusted wireless networks.

6. DOC devices remotely connecting to the Wireless Local Authorized Network (WLAN) must utilize two factor authentication.

7. Unauthenticated Internet access is not permitted on DOCs WLAN.

8. Wireless access points (AP) are limited to authorized domain users with properly configured wireless clients.

   a. A Wireless Guest Network (WGN) has been established for the purpose of providing controlled access to the Internet for users without a COV network account or for devices that are agency managed and do not allow for COV authentication.

   b. ITU Security will administer all access to the WGN, including any long-term guest access accounts for medical out-of-band equipment and users. Requested access to the WGN is provisioned by completing the *Acceptable Use Agreement for Guest of Virginia Wireless Access* 310_F9.

   c. WGN privileges will not be assigned to mobile devices (iPhones, iPads, etc.) except where a mobile device is controlled by a Mobile Device Management (e.g., MobileIron or alike) and is owned by the DOC.

   d. WGN accounts must not be shared.

   e. WGN accounts will not be utilized for student or training environments.

   f. WGN accounts will only be granted for the time period required in order to conduct official DOC business. If an extended time period is required, an exception from ITU Security must be requested or for COV users utilizing equipment that cannot be authenticated on the COV wireless network.

9. Only COV owned or leased equipment will be granted access to an internal WLAN.

10. Physical or logical separation between the WLAN and wired LAN segments must exist.

D. Encryption and data security

1. All internal IT communication that is deemed sensitive must be encrypted. VITA requires the use of data protection mechanisms (Virtru) for the transmission of all email and attached data that is sensitive.

2. VITA requires that all sensitive email (internal or external) must be encrypted (Virtru).

3. All external IT communications that is deemed sensitive that is transmitted via email will be considered sensitive. Users are reminded to consider data that will not be shared externally prior to transmitting.

4. Any new processes, protocols, or applications that pass credentials in clear text cannot be used internally and must not be used externally (examples - FTP, TELNET). Existing processes using these technologies must be remedied as soon as possible.

5. All encryption should be 128 bit or greater.

6. Sensitive documents printed to a globally shared printer must be retrieved immediately.

7. When no longer needed, shred documents and erase white or blackboards of sensitive information.

8. Electronic records must be retained in accordance with the retention requirements of the Library of Virginia.

9. Password protecting a user's network home share (W drive) or email (PST) files is not authorized without prior approval from the ISO.

E. Security Awareness Training (SAT)

1. The COV ITRM Standard SEC501requires that all state agencies establish and maintain an IT security awareness program to ensure that all individuals are aware of their security responsibilities and know how to fulfill them.

2. It is the responsibility of the Organizational Unit Heads to ensure all employees assigned a DOC IT Systems account participate in the IT SAT annually. (5-ACI-1F-07)

3. All new employees must take the IT SAT within 30 days of receiving access to DOC IT Systems.

4. If extenuating circumstances such as extended annual leave, extended sick leave, short-term disability, military leave, etc. prevent a user from meeting a required due date, the user must complete IT SAT within 30 days of their return to work.

5. Employees taking the IT SAT must utilize their DOC Windows account; failure to logon using the correct account will result in not receiving credit for the training.

6. Employees, excluding those on extended leave, failing to complete the training will be in violation of Operating Procedure 135.1, *Standards of Conduct*, and may be subject to disciplinary action.

7. Employees taking IT SAT are required to read the *DOC Information Security Agreement* contained in the training.

   a. By completing the training, the user acknowledges that they agree with all stipulations in the *DOC Information Security Agreement* and will abide by the agreement.

   b. Failure to abide by the agreement will be a violation of Operating Procedure 135.1, *Standards of Conduct*, possible user disciplinary action, and will result in non-completion of training.

F. Removal of data from hardware (including copiers), data storage devices, and media - Prior to its being surplused, transferred, traded-in, disposed of, or replaced, DOC data must be removed from all electronic media resources in accordance with *Removal of Commonwealth Data from Electronic Media (SEC514)*.

# REFERENCES

18 USC §1465, *Crimes and Criminal Procedure*

COV § 2.2-603 (F), *Authority of agency directors.*

COV §2.2-2827, *Restrictions on state employee access to information infrastructure.*

COV §18.2-372, *"Obscene" defined.*

COV §18.2-374, *Production, publication, sale, possession, etc., of obscene items.*

COV §18.2-374.1:1, *Possession, reproduction, distribution, solicitation, and facilitation of child pornography; penalty.*

COV ITRM Standard SEC501, *IT Information Security Standard* (SEC501)

COV ITRM Standard SEC514, *Removal of Commonwealth Data from Electronic Media* (SEC514)

DHRM Policy 1.75 *Use of Internet and Electronic Communications Systems*

*Office of Fleet Management Services Policies and Procedures Manual*

Operating Procedure 030.1, *Evidence Collection and Preservation*

Operating Procedure 102.3, *Background Investigation Program*

Operating Procedure 135.1, *Standards of Conduct*

Operating Procedure 310.3, *Inmate/Probationer/Parolee Access to Information Technology*

Operating Procedure 310.4, *External Users Access Control*

# ATTACHMENTS

Attachment 1, *DOC Software Applications Access Authorization*

Attachment 2, *Logon Banner*

Attachment 3, *IT System Interoperability Security Statement*

# FORM CITATIONS

*Windows Admin/System Security Agreement* 310_F1

*Windows User Account Request* 310_F2

*Windows User Information Security Agreement* 310_F3

*Windows Admin/System Account Request* 310_F4

*ITU Security Incident Report* 310_F6

*Electronic Investigation Request* 310_F8

*Acceptable Use Agreement for Guest of Virginia Wireless Access* 310_F9

*DOC System Application Request* 310_F10