Virginia Department of Corrections

Technology

Operating Procedure 310.4

External Users Access Control

Authority:
Directive 310, *Technology Management*

Effective Date: March 1, 2021

Amended:

Supersedes:
New Operating Procedure

Access: ☐ Restricted ☒ Public ☐ Inmate

ACA/PREA Standards: 5-ACI-1F-06

Content Owner:	Atron Thorne Information Security Officer	*Signature Copy on File* Signature	1/22/2021 Date
Reviewer:	Zacc Allen Chief Information Officer	*Signature Copy on File* Signature	1/22/2021 Date
Signatory:	Joseph W. Walters Deputy Director for Administration	*Signature Copy on File* Signature	1/22/2021 Date

REVIEW

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

COMPLIANCE

This operating procedure applies to all units operated by the Virginia Department of Corrections (DOC) and all persons or agencies who are not employees of the DOC who require access to DOC's information systems. Practices and procedures must comply with applicable State and Federal laws and regulations, ACA standards, PREA standards, and DOC directives and operating procedures.

Table of Contents

DEFINITIONS

Acceptable Use Agreement - A document that stipulates constraints and practices that a user must agree to for access to a corporate network, website, service, or system.

Active Directory (AD) - Microsoft's proprietary directory service. It runs on Windows Server and allows administrators to manage permissions and access to network resources. Active Directory stores data as objects. An object is a single element, such as a user, group, application or device, such as a printer.

Chief Information Officer (CIO) - The head of the DOC Corrections Information Technology Unit.

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

Data Owner - Manager responsible for policy, procedure, and practice decisions regarding data and information sensitivity, access, and protection on a DOC IT system.

Information - Processed, organized, or structured data related to employees, inmates/probationers/parolees, incidents or operational units, to include: writings of all kinds, E-mail, 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 Security Officer (ISO) - The head of ITU Security.

Information System - An integrated set of components that collects, stores, and processes data to provide information, knowledge, and digital products. Information systems are composed of four components: tasks, people, structure, and technology.

Information Technology Resource Management (ITRM) - The term used to describe the processes to plan, allocate, and control information technology resources for improving the efficiency and effectiveness of business solutions.

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 also coordinates all liaison activities with VITA Science Applications International Corporation (SAIC), and its suppliers.

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

Memorandum of Agreement (MOA) - A written agreement involving financial consideration between DOC and any entity; must be submitted to the Director of Procurement and Risk Management or designee before signature.

Memorandum of Understanding (MOU) - A written collaborative understanding without financial consideration establishing the parameters of the collaboration between DOC and any entity; must be approved by the Director of Administrative Compliance or designee before signature.

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**.**

PURPOSE

This operating procedure establishes standards for access to Department of Corrections (DOC) information systems for those persons and agencies that are external to the DOC.

PROCEDURE

I. General

A. Due to the sensitivity of the information within DOC's information systems, restricted access and special protocols are in place to ensure the information is accessed in a secure way at all times.

B. Restricted access is also necessary for DOC to meet the control requirements outlined in the Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Security Standard SEC501, Section 8.1 Access Control Family, Controls AC-1 through AC-17-COV, and AC22.Account Management

II. Authorization

1. Requests for external user access to DOC's information systems are reviewed, approved, or denied by DOC ITU Security under direction of the Chief Information Officer (CIO) and Information Security Officer (ISO), who serve as designees for the Agency Head (SEC501-11, AC-2, Account Management, Section E).
2. DOC ITU Security, under direction of the CIO and ISO, approves requests for access after confirming the following items are complete:
   a. The appropriate Memorandum of Understanding (MOU) is in place for the agency/user; see Attachment 1, *Acceptable Use Agreement for External Users*;
   b. A completed background check is on record for the agency/user;
   c. Multifactor authentication is used by the agency/user to access the systems or applications;
   d. The appropriate data owner approves the agency's/user's access;
   e. The agency's/user's business justification aligns with the user's agency, job, and role;
   f. If applicable, VITA SEC 501 requires agency's/user's access to the system and/or application; and;
   g. The Agency Head/user completed the appropriate access form and submitted a ticket for access to the DOC ISO.
3. Signed MOU's and Memorandum of Agreements are maintained and stored by the Administrative Compliance Unit; see Attachment 2, *Memorandum of Agreement*.
4. *Acceptable Use Agreement for External Users,* Attachment 1, are maintained and stored by the ISO in the Information Technology Unit (ITU).
5. Proof of background checks are stored and maintained by the Background Unit.
6. External users or agencies that may be granted access to DOC's information systems include local, state, and federal public safety agencies, the Virginia Parole Board, the state Compensation Board, jails, and other agencies and vendors that provide services to DOC, or by special arrangement.
7. All use of DOC's information systems is logged, maintained, and reviewed.

B. Least Privilege

1. Access to DOC's information systems is held to the principal of least privilege. This requires that only the privileges essential to accomplish a task are granted (SEC501-11, AC-6 Least Privilege).
2. Access and permissions are granted directly to individual users or via Commonwealth of Virginia (COV) Active Directory groups.

C. Authentication

1. Two-factor authentication and a COV account are required to access DOC's information systems.

a. Users without a COV account must request one from ITU Security via email (ctsusecurity@vadoc.virginia.gov). Users must complete and submit a completed *Windows User Information Security Agreement* 310_F3 with their email request.

b. The email should also include the name of the system/application to which the user needs access.

2. A token is required to authenticate users on the DOC network; see Operating Procedure 310.2, *Information Technology Security* for further information.

a. All requests for hard tokens must be submitted to ITU Security and approved by the IT Asset Management Team.

b. In lieu of a hard token, users with COV issued mobile phones may use the remote access mobile app to authenticate on the DOC network.

c. ITU Security requests the token through Virginia Information Technologies Agency (VITA), who in turn sends instructions to the user on how to activate the token and access the DOC portal.

D. Suspension or Termination of Access (5-ACI-1F-06)

1. The Data Owner, CIO, and ISO reserve the right to revoke access to DOC's information systems at any time.

2. Access to DOC's information systems is provided via COV Active Directory accounts to ensure all user access is terminated when a user no longer requires access to the information system. This requirement also ensures that account deactivations due to inactivity are centrally managed.

3. In cases of automated systems, written data security policy, procedure, practice govern the issuance, use, and termination of user accounts. The issuance and use of computing devices that connect to the automated information systems, the use of standalone and online applications within the information systems, and the collection, storage, retrieval, access, use, and transmission of sensitive or confidential data that resides in the information system.

E. User Access Review

1. Reviews of logins to DOC's information systems and their associated privileges are performed at least once a year (SEC501-11, AC-6 Least Privilege, (7) Least Privilege, Review of User Privileges).

2. Inactive COV Active Directory accounts are suspended via the established VITA and agency policies.

REFERENCES

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

Operating Procedure 310.2, *Information Technology Security*

ATTACHMENTS

Attachment 1, *Acceptable Use Agreement for External Users*

Attachment 2, *Memorandum of Agreement*

FORM CITATIONS

Windows User Information Security Agreement 310_F3