

Policy and Procedure 9-14

Information Security: Personnel Security

DocuSigned by:

Issued By: Robert W. Farrell, State Forester *Robert W. Farrell* 7/9/2024

2115C3D38FCF4E7...

Effective Date: June 26, 2024

Codes/Mandates: Code of Virginia, [§2.2-2005](#) Creation of Agency; appointment of Chief Information Officer
Code of Virginia: [§2.2-2007](#) Powers of the CIO

References: [Commonwealth Information Technology Resource Management \(ITRM\) Information Security Policy SEC 519-00](#),
[Commonwealth ITRM Standard SEC502: Audit Security Standard](#)
[Commonwealth ITRM Standard SEC530: Information Security Standard](#)
[DHRM Policy 1.75 Use of Electronic Communications and Social Media](#)

Forms: N/A

CONTENTS

PURPOSE	1
SCOPE	1
DEFINITIONS and ACRONYMS	2
BACKGROUND	2
ROLES & RESPONSIBILITY	2
STATEMENT OF POLICY	3
Personnel Screening (PS-3).....	3
Personnel Termination (PS-4).....	3
Personnel Transfer (PS-5).....	3
Access Agreements (PS-6)	4
External Personnel Security (PS-7).....	4
Personnel Sanctions (PS-8).....	4
Position Descriptions (PS-9)	4
AUTHORITY	5
INTERPRETATION	5
APPROVAL	5
VERSION HISTORY	5

PURPOSE

The purpose of this policy and procedure is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that Department of Forestry develops, disseminates, and updates the Information Security: Personnel Security Policy and Procedure. This policy and procedure establishes the minimum requirements for this policy and procedure.

This policy and procedure is intended to meet the control requirements outlined in SEC530, Section 8.13 Personnel Security Family, controls PS-1 through PS-8 as well as additional Commonwealth of Virginia controls.

SCOPE

All Department of Forestry employees (classified, hourly, or business partners) as well as all Department of Forestry systems classified as sensitive.

DEFINITIONS and ACRONYMS

“Agency” and “DOF” means the Virginia Department of Forestry.

“Data owner” means the agency manager or supervisor, designated by the state forester, who defines, manages and controls the use of data and ensures compliance with adopted standards.

“Information security officer” and “ISO” means the agency employee who is designated by the state forester to develop and manage the agency’s information security program, as required in the Commonwealth’s Information Security Standard, SEC530.

“System administrator” means the agency employee who implements, manages, and/or operates a system at the direction of the system owner or data owner.

“System owner” means the agency manager or supervisor who is responsible for the operation and oversight of any given agency business system.

ACRONYMS

CIO:	Chief Information Officer
COV:	Commonwealth of Virginia
CSRM:	Commonwealth Security and Risk Management
DOF:	Department of Forestry
ISO:	Information Security Officer
IT:	Information Technology
ITRM:	Information Technology Resource Management
SEC530:	Information Security Standard 530
VITA	Virginia Information Technology Agency

BACKGROUND

The Information Security: Personnel Security Policy and Procedure at Department of Forestry is intended to facilitate the effective implementation of the processes necessary to meet the personnel security requirements as stipulated by the COV ITRM Security Standard SEC530 and security best practices. This policy directs that Department of Forestry meet these requirements for all sensitive IT systems.

ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibility as described in the Statement of Process section. The following Roles and Responsibility Matrix describes 4 role specific activities:

- ◆ Responsible (R) – Person working on activity
- ◆ Accountable (A) – Person with decision authority and one who delegates the work
- ◆ Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
- ◆ Informed (I) – Person who needs to know of decision or action

Roles	Users	User Supervisor	System Owner	System Admin	Information Security Officer
Tasks					
Require screening of individuals.					A

Terminate access and retrieve all organizational property upon termination.		R			A
Review and modify logical and physical access authorizations when personnel are reassigned or transferred.		A		R	
Sign appropriate access agreements.	R				A
Review and update access agreements.					A/R
Establish and document personnel security requirement for third-party providers.					A/R
Employ a formal sanction process.					A/R

STATEMENT OF POLICY

In accordance with SEC530, PS-1 through PS-9, DOF shall protect sensitive information and information systems by requiring specific procedures for personnel pre-employment, employment, and post-employment.

Personnel Screening (PS-3)

1. The ISO shall require that:
 - a. Individuals must undergo background screening prior to being authorized access to the information system.
 - b. Individuals must be rescreened if the length of employment separation exceeds 90 days.
 - c. Personnel screening and rescreening must be consistent with applicable state laws, directives, policies, regulations, standards, guidance and the criteria established for the risk designation of the assigned position.

Personnel Termination (PS-4)

1. The ISO shall require upon termination of individual employment:
 - a. Information system access is disabled:
 - i. If termination is voluntary (i.e., normal, scheduled), terminate information system access within the same day of notification of such termination (i.e., same day the individual is terminated).
 - ii. If termination is involuntary (i.e., emergency, adverse), terminate information system access within 24 hours of notification of such termination (i.e., same day the employee is terminated).
 - b. All authenticators and credentials associated with the individual are revoked or terminated.
 - i. Collect all keys, badges, and similar items.
 - c. All security-related organizational information system-related property is retrieved (e.g., hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes).
 - d. Access to organizational information and information systems formerly controlled by terminated individual is retained.
 - i. Prior to archiving or permanent disabling of accounts, transfer all DOF information to appropriate personnel or archives.
 - ii. In the event of an adverse removal or involuntary termination, rotate the employee or contractor to a non-sensitive position or restrict access or rights to information systems before notification, whenever possible, to avoid the potential for malicious actions to information systems.

Personnel Transfer (PS-5)

Note: This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted.

1. The ISO shall require that:

- a. Logical and physical access authorizations to information systems and facilities must be reviewed when personnel are reassigned or transferred to other positions within DOF and the appropriate actions must be initiated.
- b. The transfer or reassignment actions must be initiated within 24 hours following the formal transfer action.
- c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.
- d. Notify the appropriate organization-defined personnel within organization defined time period.

Access Agreements (PS-6)

1. The ISO requires that:
 - a. [DHRM Policy 1.75 Use of Electronic Communications and Social Media](#) must be signed by individuals requiring access to DOF information and information systems prior to being granted access.
 - i. Signed access agreements must include an acknowledgement that individuals have read, understand and agree to abide by the constraints associated with the information system to which access is authorized.
 - ii. Access agreements must state that penalties for non-compliance may include sanctions and possible criminal and/or civil prosecution.
 - b. The access agreements must be reviewed and updated (i.e., redistributed and signatures collected) as follows:
 - i. On an annual basis.
 - ii. Whenever there is a significant change to the information system or information being processed.
 - iii. Whenever there is a change to the agreements' verbiage.

Note: Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by Agency policy.

External Personnel Security (PS-7)

1. The ISO shall require:
 - a. Personnel security requirements including security roles and responsibilities for external providers (e.g., service bureaus, contractors and other organizations providing information system development, information technology services, outsourced applications and network and security management) must be established.
 - b. Personnel security requirements must be documented.
 - i. Personnel security requirements must be explicitly included in acquisition-related documents.
 - c. Require external providers to notify the appropriate organization-defined personnel of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within 24 hours or immediately for high-risk individuals.
 - d. Provider compliance with personnel security requirements must be monitored.

Personnel Sanctions (PS-8)

1. The ISO shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.
 - a. The sanctions process must be consistent with applicable state laws, directives, policies, regulations, standards, and guidance where applicable.

Position Descriptions (PS-9)

1. The ISO shall require:

- a. Security and privacy roles and responsibilities will be incorporated into organizational position descriptions to facilitate clarity in understanding the security or privacy responsibilities associated with the roles and the role-based security and privacy training requirements for the roles.

AUTHORITY

This policy and procedure is issued by the Virginia state forester.

INTERPRETATION


The director of information technology and the chief of administration are responsible for the interpretation of this policy and procedure.

APPROVAL

I certify that this policy and procedure is approved and ready for publication.

Parik Patel

Director of Information Technology Name (Print)

DocuSigned by:
 7/2/2024
3448F7C5358F457
 Director of Information Technology Signature

Amanda Davis

Chief of Administration Name (Print)

DocuSigned by:
 7/9/2024
C2CCAB00F65A4A0
 Chief of Administration Signature

VERSION HISTORY

Version History			
Date	Version	Details	Author/Contributors
June 26, 2024	1	Original – CSRM template and updated with SEC530	Catherine Shefski, ISO