# Policy and Procedure 9-12
# Information Security: Planning

| | | | |
|---|---|---|---|
| **Issued By:** | Robert W. Farrell, State Forester | DocuSigned by: Robert W. Farrell 2115C3D38FCF4E7... | 6/24/2024 |
| **Effective Date:** | June 13, 2024 | | |
| **Codes/Mandates:** | Code of Virginia, §2.2-2005 Creation of Agency; appointment of Chief Information Officer<br>Code of Virginia: §2.2-2007 Powers of the CIO | | |
| **References:** | Commonwealth Information Technology Resource Management (ITRM) Information Security Policy SEC 519-00,<br>Commonwealth ITRM Standard SEC502: Audit Security Standard<br>Commonwealth ITRM Standard SEC530: Information Security Standard<br>Department of Human Resource Management (DHRM) Policy 1.75 Use of Electronic Communications and Social Media | | |
| **Forms:** | N/A | | |

## CONTENTS



## PURPOSE

The purpose of this policy 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 Planning Policy and Procedure. This policy and procedure establishes the minimum requirements for the Information Security Planning Policy and Procedure.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.12 Planning Family, controls PL-1, PL-2, PL-4, PL-8, PL-9, PL-10 and PL-11 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 |
| DoS: | Denial of Service |
| ISO: | Information Security Officer |
| IT: | Information Technology |
| ITRM: | Information Technology Resource Management |
| LAN: | Local Area Network |
| ROB: | Rules of Behavior |
| SEC530: | Information Security Standard 530 |
| SSP: | System Security Plan |
| VCCC: | VITA Customer Care Center |
| VITA | Virginia Information Technology Agency |

# BACKGROUND

The Information Security: Planning Policy and Procedure at Department of Forestry is intended to facilitate the effective implementation of the processes necessary to meet the IT system security planning 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 | System Owner | System Admin | Information Security Officer |
|---|---|---|---|---|
| **Tasks** | | | | |
| Develop a system security plan. | | A | | I |
| Review and update security plan. | | A | | R |
| Plan, document and implement additional security controls. | | A | R | R |
| Validate and verify compliance. | | | | A |
| Establish rules of behavior. | I | I | | A/R |
| Receive signed acknowledgement from users for rules of behavior. | R | I | | A |
| Plan and coordinate security-related activities. | | A | R | R |

# STATEMENT OF POLICY

In accordance with SEC530, section 8.12 Planning, PL-1 through PL-11 and additional requirements for the Commonwealth of Virginia, Department of Forestry shall develop and implement a system security plan for each information system classified as sensitive. DOF shall establish a set of rules to address a user's expected behavior with regard to sensitive information and information system usage. DOF shall plan and coordinate security-related activities affecting these information systems.

## System Security and Privacy Plan (PL-2)

1. The system owner in collaboration with ISO shall develop a system security and privacy plan (SSP) that describes the processes, procedures and security requirements, and describes the security controls in place or planned for meeting those requirements. The system security plan must adhere to the following requirements:
    a. Consistent with Department of Forestry's enterprise architecture.
    b. Explicitly defines the constituent system component.
    c. Describes the operational context of the information system in terms of mission and business processes.
    d. Identifies the individuals that fulfill system roles and responsibilities.
    e. Identifies the information types processed, stored and transmitted by the system.
    f. Provides the security categorization of the information system, including supporting rationale.
    g. Describes any specific threats to the system that are of concern to DOF.
    h. Describes the operational environment for the information system and any dependencies on or connections to other systems or system components.
        i. All IT assets, including hardware, software, and (if appropriate) networking/ telecommunications equipment, must be listed and described.
        ii. The description must reflect any environmental or technical factors that are of security significance (e.g., versions, protocols, ports, wireless technology, public access, hosting or operation at a facility outside of the organization's control), as applicable.
        iii. The description must include applicable diagrams (e.g., network diagrams, system boundary, interconnections, data flow, and high-level design).
    i. Provides an overview of the security and privacy requirements for the system.

j. Identifies any relevant control baselines or overlays, if applicable.

k. Completed based on the results of the risk assessment and describes how existing or planned security controls provide adequate mitigation of risks to which the IT system is subject.

l. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions and a schedule for implementing planned controls.

m. Reviewed and approved by the agency head or ISO prior to plan implementation.

2. The ISO shall distribute copies of the plans and communicate changes to the plans to appropriate agency personnel.

3. The system owner and ISO shall update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

   a. The SSP must be updated when impacted by unforeseen significant events, such as a breach, a new threat, or previously unknown vulnerability.

   b. The SSP must be updated when there is a significant change to the system, including a change in the points of contact, system architecture, system status, system interconnections, or system scope.

   c. The SSP must be updated to factor in planned information system enhancements, to ensure that required security-related activities are planned for in advance.

4. The system owner shall protect the plans from unauthorized disclosure and modification.

5. The system owner shall plan, document, and implement additional security controls for the IT system if the agency head or designated ISO disapproves the IT SSP, and resubmit the IT SSP to the agency head or designated ISO for approval.

6. The ISO is responsible for verifying and validating compliance with the provisions of this policy.

## Rules of Behavior (ROB) (PL-4)

1. The ISO or designee shall:

   a. Establish and make readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and system usage, security and privacy.

      i. The ROB must include general rules for all users and targeted rules for specific functions such as information system administration, developers, end users, etc.

   b. Receive documented acknowledgment from users indicating that they have read, understand, and agree to abide by the ROB before authorizing access to information and the information system.

      i. Electronic signatures are acceptable for use in acknowledging ROB.

   c. Review and update the ROB at least on an annual basis and following an environmental change.

   d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are revised or updated.

   e. Include in the ROB restrictions on:

      i. The use of social media, social networking sites and external sites/applications.

      ii. Posting organizational information on public websites.

      iii. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

   f. Document a DOF acceptable use policy which adheres to Virginia Department of Human Resource Management (DHRM) Policy 1.75 Use of Electronic Communications and Social Media and is supplemented as needed by DOF, which shall prohibit users from:

      i. Installing or using proprietary encryption hardware/software on COV systems.

ii. Tampering with security controls or tools to inventory hardware or software configured on COV workstations.

iii. Installing personal software on a COV system.

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

v. Connecting non-COV-owned devices to a COV IT system or network, such as personal computers, laptops, or hand-held devices, except in accordance with the current version of the Use of non-Commonwealth Computing Devices to Telework Standard (COV ITRM Standard SEC511).

g. Prohibit storing, using or transmitting copyrighted and licensed materials on COV systems unless the COV owns the materials or COV has otherwise complied with licensing and copyright laws governing the materials.

h. Consult with legal counsel when considering adopting an email disclaimer. Emails sent from DOF systems are public records of the Commonwealth of Virginia and must be managed as such.

i. Prohibit the installation or use of software that may cause harm to the commonwealth as identified by Commonwealth Security and Risk Management.

## Security and Privacy Architecture (PL-8)

1. The ISO or designee in coordination with the system owner shall:

   a. Develop security and privacy architecture for the system that:

      i. Describes the requirements and approach to be taken for protecting the confidentiality, integrity and availability of organizational information.

      ii. Describes how the architectures are integrated into and support the enterprise architecture.

      iii. Describes any assumptions about and dependencies on, external systems and services.

   b. Review and update the architectures at least on an annual basis and following an environmental change to reflect changes in the enterprise architecture.

   c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

   d. Design the security and privacy architectures for the system using a defense-in-depth approach that:

      i. Allocates organization-defined controls to organization-defined locations and architectural layers.

      ii. Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.

   e. Require that organization-defined controls allocated to organization-defined locations and architectural layers are obtained from different suppliers.

## Central Management (PL-9)

**Note:** Central management refers to organization-wide management and implementation of selected controls and processes. This includes planning, implementing, assessing, authorizing and monitoring the organization-defined, centrally managed controls and processes. As the central management of controls is generally associated with the concept of common (inherited) controls, such management promotes and facilitates standardization of control implementations and management and the judicious use of organizational resources. Centrally managed controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate and as part of organizational continuous monitoring.

- The system owner shall centrally manage organization-defined controls and related processes.

## Baseline Selection (PL-10)

**Note:** Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws,

executive orders, directives, regulations, policies, standards and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information and information systems with subsequent tailoring actions to manage risk in accordance with mission, business or other constraints (see PL-11).

- The system owner shall select a control baseline for the system

### Baseline Tailoring (PL-11)

**Note:** The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. Tailoring actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific mission and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems and any other conditions or situations that can impact their mission or business success. Tailoring guidance is provided in [SP 800-53B]. Tailoring a control baseline is accomplished by identifying and designating common controls, applying scoping considerations, selecting compensating controls, assigning values to control parameters, supplementing the control baseline with additional controls as needed and providing information for control implementation.

- The system owner shall tailor the selected control baseline by applying specified tailoring actions.

## 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 | DocuSigned by: Parik Patel 3448F7C5358F457... | 6/13/2024 |
| Director of Information Technology Name (Print) | Director of Information Technology Signature | |
| Amanda Davis | DocuSigned by: amanda davis C2CCAB60F85A4A6... | 6/13/2024 |
| Chief of Administration Name (Print) | Chief of Administration Signature | |

## Version History

| Version History | | | |
|---|---|---|---|
| **Date** | **Version** | **Details** | **Author/Contributors** |
| June 13, 2024 | 1 | Original – CSRM template and updated with SEC530 | Catherine Shefski, ISO |