Policy and Procedure 9-13
Information Security: Program Management

DocuSigned by:
Robert W. Farrell
2115C3D38FCF4E7...

Issued By:	Robert W. Farrell, State Forester	7/9/2024
Effective Date:	June 28, 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	
Forms:	N/A	

CONTENTS

PURPOSE

The purpose of this policy and procedure is to facilitate the effective implementation of the security program management requirements as stipulated by the COV ITRM Security Standard SEC530, Section 8.13 Program Management, PM-1 through PM-32, and security best practices.

SCOPE

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

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

ACRONYMS

BIA:	Business Impact Analysis
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
PII:	Personally Identifiable Information
ITRM:	Information Technology Resource Management
RA:	Risk Assessment
SEC530:	Information Security Standard 530
SSP:	System Security Plan
VCCC:	VITA Customer Care Center
VITA:	Virginia Information Technology Agency

BACKGROUND

The Information Security Program Management Policy and Procedure is intended to facilitate the effective implementation of the security program management requirements as stipulated by the COV ITRM Security Standard SEC530, Section 8.13 Program Management, PM-1 through PM-32, and security best practices.

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	Agency Head	Director of IT	System Owner	Information Security Officer
Tasks				
Appoint an information security officer.	R/A	I		I
Oversee resource allocation and documentation for DOF information security programs.		R/A		
Require, document, and review DOF plans of action and milestones for DOF systems.			R	R/A
Maintain an inventory of organizational systems, updated annually.				R/A
Record, monitor and report on DOF measures of performance for information security.	I	I		R/A
Develop and maintain enterprise architecture with consideration for information security.		R/A		
Address information security in the development, documentation and updating of the DOF contingency plan.				R/A
Develop a comprehensive risk management strategy for DOF information systems.				R/A
Manage the security of IT systems through authorizations processes.		R/A		
Complete BIA and RA for DOF sensitive systems and update annually.		R/A	C	R/A
Utilize VITA ISO services for support of security workforce development.		R/A		I
Implement DOF plans for testing, training and monitoring of IT systems.				R/A
Minimize PII in testing, training and research.	R/A	R		R
Develop, distribute, review and update the BIA, RA and SSP for DOF sensitive systems.	C			R/A
Analyze DOF systems for support of mission essential services or functions.		R/A		

STATEMENT OF POLICY

In accordance with SEC530, Section 8.13 Program Management, PM-1 through PM-32, DOF shall create an organization-wide information security program plan providing an overview of the security program and a description of the management and common controls in place to meet the requirements. This plan will be reviewed and updated on an annual basis or when environmental or organizational changes occur.

Information Security Program Leadership Role (PM-2)

1. The agency head will appoint an information security officer with the mission and resources to coordinate, develop, implement and maintain an organization-wide information security program.

Information Security And Privacy Resources (PM-3)

1. The director of IT shall:

   a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement.

   b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations and standards.

   c. Make the planned information security and privacy resources available for expenditure.

Plan Of Action And Milestones Process (PM-4)

1. The ISO shall:

a. Require plans of action and milestones, as described in (PP_9_04, CA-5), to be developed and maintained by system owners, including an annual review and updates as needed or due to environmental changes.

b. Document and report remediation actions for information security risk management in accordance with current VITA guidelines.

c. Review plans of action and milestones for consistency with the DOF risk management strategy and priorities for risk response actions.

System Inventory (PM-5)

1. The ISO shall maintain an inventory of DOF systems to be updated on an annual basis including all systems, applications and projects that process personally identifiable information (PII).

Measures Of Performance (PM-6)

1. The ISO shall:

a. Enter required measures of performance into Archer.

b. Monitor the DOF risk score and DOF audit score.

c. Report on the results of information security and privacy measures of performance to DOF director of IT and agency head.

Enterprise Architecture (PM-7)

1. The director of IT will develop and maintain an enterprise architecture with consideration for information security, privacy and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

Critical Infrastructure Plan (PM-8)

1. The ISO will address information security and privacy issues in the development, documentation and updating of a contingency plan (critical infrastructure and key resources protection) (see CP-2, CP-4 in PP_9_06).

Risk Management Strategy (PM-9)

1. The ISO shall:

a. Develop a comprehensive strategy to manage:

i. Security risk to organizational operations and assets, individuals, other organizations and the Nation associated with the operation and use of organizational systems.

ii. Privacy risk to individuals resulting from the authorized processing of PII.

b. Implement the risk management strategy consistently across the organization.

c. Review and update the risk management strategy at least on an annual basis or as required, to address organizational changes.

Authorization Process (PM-10)

1. The director of IT shall:

a. Manage the security and privacy state of DOF systems and the environments in which those systems operate through authorization processes.

b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process.

c. Integrate the authorization processes into an organization-wide risk management program.

Mission And Business Process Definition (PM-11)

1. The ISO will work with the director of IT and system owners to:
    a. Complete a business impact analysis and a risk assessment for each sensitive system to define DOF mission and business processes with consideration for information security and privacy and the resulting risk to DOF operations, assets, individuals, other organizations and the Nation.
    b. Determine information protection and PII processing needs arising from the defined mission and business processes.
    c. Review and revise the mission and business processes for each sensitive system at least on an annual basis.

Security And Privacy Workforce (PM-13)

1. Director of IT and ISO will utilize VITA ISO services to support security and privacy workforce development and improvement.

Testing, Training, And Monitoring (PM-14)

1. The ISO will:
    a. Implement a process for ensuring that DOF plans for conducting security and privacy testing, training and monitoring activities associated with organizational systems:
        i. Are developed and maintained.
        ii. Continue to be executed.
    b. Review testing, training and monitoring plans for consistency with the DOF risk management strategy and DOF priorities for risk response actions.

Minimization Of Personally Identifiable Information Used In Testing, Training and Research (PM-25)

1. DOF will avoid using PII for internal testing, training and research.
2. If needed, the agency head will authorize the use of PII when such information is required for internal testing, training and research.
3. The ISO will review and update policies and procedures for the use of PII for internal testing, training and research on an annual basis.

Risk Framing (PM-28)

1. The ISO will:
    a. Develop the Business Impact Analysis (BIA), Risk Assessment (RA), and System Security Plan (SSP) for each of DOF’s sensitive systems in order to identify and document:
        i. Assumptions affecting risk assessments, risk responses, and risk monitoring.
        ii. Constraints affecting risk assessments, risk responses, and risk monitoring.
        iii. Priorities and trade-offs considered by the organization for managing risk.
        iv. Organizational risk tolerance.
    b. Distribute results of risk framing to system owners and the agency head with approval of BIA, RA, and SSP from the agency head.
    c. Review and update the RA and SSP for all DOF sensitive systems on an annual basis.

Continuous Monitoring Strategy (PM-31)

1. The ISO will develop a DOF continuous monitoring strategy and implement continuous monitoring programs that include:
   a. Establishing the monitoring of DOF's: risk mitigation, vulnerabilities, audit record coverage and other organization-defined metrics.
   b. Establishing at least on a monthly basis for monitoring and at least on a quarterly basis for assessment of control effectiveness.
   c. Ongoing monitoring of organizationally defined metrics in accordance with the continuous monitoring strategy.
   d. Correlation and analysis of information generated by control assessments and monitoring.
   e. Response actions to address results of the analysis of control assessment and monitoring information.
   f. Reporting the security and privacy status of DOF systems to the director of IT on a monthly basis.

Purposing (PM-32)

1. The director of IT will analyze DOF systems or system components supporting mission essential services or functions to ensure that the information resources are being used consistently with their intended purpose.

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:
Parik Patel
3448F7C5358F457...
7/2/2024
Director of Information Technology Signature

Amanda Davis
Chief of Administration Name (Print)

DocuSigned by:
amanda davis
C2CCAB60F85A4A6...
7/9/2024
Chief of Administration Signature

Version History

Version History			
Date	**Version**	**Details**	**Author/Contributors**
June 28, 2024	1	Original – CSRM template and updated with SEC530	Catherine Shefski, ISO