Policy and Procedure 9-4
Information Security: Assessment, Authorization and Monitoring

Issued By:	Robert W. Farrell, State Forester	DocuSigned by: Robert W. Farrell 2115C3D38FCF4E7...	6/5/2024
Effective Date:	May 23, 2024		
Codes/Mandates:	Code of Virginia: §2.2-2007 and Code of Virginia, §2.2-2005		
References:	Commonwealth Information Technology Resource Management (ITRM) Information Security Policy SEC 519-00, ITRM Standard SEC530: Information Security Standard, ITRM Standard SEC502: Audit Security Standard		
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 standard, to ensure that Department of Forestry develops, disseminates, and updates the Assessment, Authorization and Monitoring policy and procedure. This policy and procedure establishes the minimum requirements for the Assessment, Authorization and monitoring controls.

This policy is intended to meet the control requirements outlined in SEC530, Section 8.4 Security Assessment and Authorization Family, Controls CA-1 through CA-9, to include specific requirements for the Commonwealth of Virginia.

SCOPE

All Department of Forestry employees (classified, hourly, or business partners) as well as all Department of Forestry information and information systems including systems used or operated by contractors and other third parties on behalf of Department of Forestry.

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
ISO:	Information Security Officer
IT:	Information Technology
ITRM:	Information Technology Resource Management
SEC530:	Information Security Standard 530
DOF:	Department of Forestry

BACKGROUND

The security assessment and authorization program at Department of Forestry is intended to ensure that necessary security controls are integrated into systems and processes within Department of Forestry. This policy directs that Department of Forestry meet the requirements as stipulated by COV ITRM Security Standard SEC530 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	User	User Manager	System Owner	System Admin	Information Security Officer
Tasks					
Review and update policy					A/R
Responsible for documentation and/or interconnection Security Agreement (ISA) of dedicated connections between information systems			A	R	I
Assign an authorizing official for each system					A/R
Establish a continuous monitoring strategy					A/R

STATEMENT OF POLICY

In accordance with SEC530, Controls CA-1 through CA-9, Security Assessment and Authorization controls, Department of Forestry ISO will develop, disseminate, and review/update the Security Assessment, Authorization and Monitoring Policy and Procedure on an annual basis or more frequently if an environmental change is made to a system involved in an interconnection agreement.

Security Assessments (CA-2)

Organizations assess controls in systems and the environments in which those systems operate as part of initial and ongoing authorizations, continuous monitoring, FISMA annual assessments, system design and development, systems security engineering, privacy engineering and the system development life cycle. Assessments help to ensure that organizations meet information security and privacy requirements, identify weaknesses and deficiencies in the system design and development process, provide essential information needed to make risk-based decisions as part of authorization processes and comply with vulnerability mitigation procedures.

1. DOF will select an appropriate assessor or team for the type of assessment conducted.
2. Develop a control assessment plan that describes the scope of the assessment including:.
    a. Controls and control enhancements under assessment
    b. Assessment procedures to be used to determine control effectiveness
    c. Assessment environment, assessment team, and assessment roles and responsibilities
3. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment.
4. Assess the controls in the system and its environment of operation at least on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements.
5. Produce a control assessment report that document the results of the assessment.
6. Provide the results of the control assessment to the ISO and any other organization-defined individuals.

Information Exchange (CA-3)

This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing.

1. Connections from the information system to other information systems outside of the authorization boundary must be authorized by the system owner through the use of Interconnection Security Agreements (ISAs).
    a. If the connecting systems have the same authorizing official, an ISA is not required. Rather, the interface characteristics between the connecting information systems must be described in the security plans for the respective systems.
    b. If the connecting systems have different authorizing officials but the authorizing officials are in the same organization, DOF shall determine whether an ISA is required, or alternatively, the interface characteristics between the connecting information systems must be described in the security plans for the respective systems.
        - **NOTE:** Instead of developing an ISA, organizations may choose to incorporate this information into a formal contract, especially if the connection is to be established between an agency and a non-Commonwealth (i.e., private sector) organization. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the connection of the information systems.

Plan of Action and Milestones (CA-5)

1. For every sensitive agency IT system that shares data with non-Commonwealth entities, the agency shall require or shall specify that its service provider require:
    a. The system owner, in consultation with the data owner, shall document IT systems with which data is shared. This documentation must include:
        i. The types of shared data.
        ii. The direction(s) of data flow.
        iii. Contact information for the organization that owns the IT system with which data is shared, including the system owner, the ISO or equivalent and the system administrator.
    b. The system owners of interconnected systems must inform one another of connections with other systems.
    c. The system owners of interconnected systems must notify each other prior to establishing connections to other systems.
    d. The written agreement shall specify if and how the shared data will be stored on each IT system.
    e. The written agreement shall specify that system owners of the IT systems that share data acknowledge and agree to abide by any legal requirements (i.e., HIPAA) regarding handling, protection and disclosure of the shared data, including but not limited to, data breach requirements in the Information Security Standard SEC530.
    f. The written agreement shall specify each data owner's authority to approve access to the shared data.
    g. The system owners shall approve and enforce the agreement.
2. Risks that may be introduced when information systems are connected to other systems with different security requirements and security controls must be carefully considered. The authorizing official shall determine the risk associated with each connection and the appropriate controls to be employed.

Authorization (CA-6)

Authorizations are official management decisions by senior officials to authorize operation of systems, authorize the use of common controls for inheritance by organizational systems, and explicitly accept the risk to organizational operations and assets, individuals, other organizations and the Nation based on the implementation of agreed-upon controls.

For each information system, the ISO or designee shall:

1. Assign a senior-level executive or manager to the role of authorizing official for the information system;
    a. Authorizing officials typically have budgetary oversight for information systems or are responsible for the mission or business operations supported by the systems.
    b. Security authorization is an inherently Commonwealth responsibility and therefore, authorizing officials must be Commonwealth employees.
    c. Through the security authorization process, authorizing officials are accountable for the security risks associated with information system operations. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks.
2. Ensure that the authorizing official authorizes the information system for processing before commencing operations; and
3. Update the security authorization at least once a year.
    a. Through the employment of a comprehensive continuous monitoring process, the critical information contained in the authorization package (i.e., the security plan (including risk assessment), the security assessment report and the plan of action and milestones) is updated on an ongoing basis, providing the

authorizing official and the information system owner with an up-to-date status of the security state of the information system.

b. To reduce the administrative cost of security reauthorization, the authorizing official uses the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision.

Continuous Monitoring (CA-7)

A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies and missions/business processes.

Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system.

1. The ISO or designee shall establish a continuous monitoring strategy and implement a continuous monitoring program that includes:
    a. Monitoring DOF system-level metrics.
    b. Establishing organization-defined frequencies for monitoring and organization-defined frequencies for assessment control effectiveness.
    c. Ongoing control assessments in accordance with the continuous monitoring strategy.
    d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy. Metrics include operating system scans on a monthly basis, database and web application scans on a monthly basis and independent assessor scans performed annually.
    e. Correlation and analysis of information generated by control assessments and monitoring.
    f. Response actions to address results of the analysis of control assessments and monitoring information.
    g. Reporting the security and privacy status of the system to appropriate organizational officials at least every 120 days.
    h. Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities and the types of activities used in the continuous monitoring process need to be modified based on empirical data.
    i. Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:
        i. Effectiveness monitoring.
        ii. Compliance monitoring.
        iii. Change monitoring.
    j. Ensure the accuracy, currency, and availability of monitoring results for the system using organization-defined automated mechanisms.

Penetration Testing (CA-8)

DOF will conduct penetration testing on an annual basis and following an environmental change on any system housing Commonwealth data.

Internal System Connections (CA-9)

Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors and servers. Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners and copiers with a specified

processing, transmission and storage capability or smart phones and tablets with a specific baseline configuration. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.

The ISO or designee shall:

1. Authorize internal connections of organization-defined system components or classes of components to the system.
2. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated.
3. Terminate internal system connections after organization-defined conditions.
4. Review organization-defined frequency for the continued need for each internal connection.

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...	5/31/2024
Director of Information Technology Name (Print)	Director of Information Technology Signature	
Amanda Davis	DocuSigned by: amanda davis C2CCAB60F85A4A6...	5/31/2024
Chief of Administration Name (Print)	Chief of Administration Signature	

VERSION HISTORY

Version History			
Date	**Version**	**Details**	**Author/Contributors**
May 23, 2024	1	Original – CSRM template and updated with SEC530	Catherine Shefski, ISO