Policy and Procedure 9-16
Information Security: Risk Assessment

Issued By:	Robert W. Farrell, State Forester DocuSigned by: Robert W. Farrell 2115C3D38FCF4E7...	7/9/2024
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	
Forms:	N/A	

CONTENTS

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: Risk Assessment Policy and Procedure. This policy and procedure establishes the minimum requirements.

This policy is intended to meet the control requirements outlined in SEC520 and SEC530, Section 8.16 Risk Assessment Family, controls RA-1 through RA-10 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
CISO:	Chief Information Security Officer of the Commonwealth
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
RA:	Risk Assessment
SEC520:	Information Security Risk Management Standard
SEC530:	Information Security Standard 530
SSP:	System Security Plan
VITA:	Virginia Information Technology Agency

BACKGROUND

The Information Security: Risk Assessment Policy and Procedure is intended to facilitate the effective implementation of the processes necessary to meet the risk assessment requirements as stipulated by the COV ITRM Security Standard SEC530, COV ITRM Risk Management Standard SEC520, and security best practices. This policy and procedure directs that Department of Forestry to 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	VITA	Agency Head	System Owner	System Admin	Information Security Officer
Tasks					
Categorize and document information and information systems.	I		A/R		C
Include the system categorization in the SSP.	I		A/R		C
Review the security categorization on an annual basis.	I		A/R		C
Conduct and document assessment of risk.	C				A/R

Review and update risk assessment.	C				A/R
Create a risk finding.	I				A/R
Create a risk treatment plan.	I				A/R
Submit a Risk Assessment Plan and Risk Treatment Plan to the CISO.	I	A			I
Receive reports from the risk register and verify implementation.	I	A			R
Verify and validate compliance.					A/R
Scan and analyze information systems and hosted applications for vulnerabilities.	I		A	R	R
Remediate vulnerabilities.	I		A	R	R
Review audit logs.	I		A	R	R
Document and report vulnerabilities and risks to CISO.	I	A			I

STATEMENT OF POLICY

In accordance with SEC520 and SEC530, RA-1 through RA-10, security categorization, risk assessments, and vulnerability scans shall be used for the execution, development and implementation of remediation programs at Department of Forestry.

Security Categorization (RA-2)

1. The ISO shall require that:
    a. Information systems and the information IT processes, stores and transmits must be categorized in accordance with Commonwealth policies and procedures:
        i. The authorization boundary is a prerequisite and must be clearly defined before beginning the security categorization.
        ii. Security categorization describes the potential adverse impacts to DOF operations, DOF assets and individuals should the information and information system be comprised through a loss of confidentiality, integrity or availability.
        iii. An impact-level prioritization of organizational systems must be conducted to obtain additional granularity on system impact levels.
    b. Security categorization results must be documented (including supporting rationale) in the system security plan (SSP) for the information system.
    c. Verification is made that the authorizing official/designee reviews and approves the security categorization decision.

Risk Assessment (RA-3)

1. The ISO must enforce the following Risk Assessment requirements for each IT system classified as sensitive including:
    a. Conduct a risk assessment, including:
        i. Identifying threats to and vulnerabilities in the system.
        ii. Determining the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the system, the information it processes, stores, or transmits, and any related information.
        iii. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.
    b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments.

c. Document risk assessment results in a risk assessment report.

d. Review risk assessment results at least on an annual basis and following an environmental change.

e. Disseminate risk assessment results to the appropriate organization-defined personnel.

f. Update the risk assessment on an annual basis or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

g. Assess supply chain risks associated with high-risk systems, high-risk system components and cloud-based service providers.

h. Update the supply chain risk assessment at least on an annual basis, when there are significant changes to the relevant supply chain or when changes to the system, environments of operation or other conditions may necessitate a change in the supply chain.

i. Use all-source intelligence to assist in the analysis of risk.

j. Determine the current cyber threat environment on an ongoing basis using threat information provided by Commonwealth Security and Risk Management.

2. Risk assessments consider vulnerabilities, threat sources and security controls planned or in place to determine the level of residual risk posed to organizational operations and assets, individuals, other organizations, and the Commonwealth based on the operation of the information system.

   a. Risk assessments also take into account risk posed to DOF operations, DOF assets or individuals from external parties, including but not limited to:

      i. Service providers.

      ii. Contractors operating information systems on behalf of the organization.

      iii. Individuals accessing DOF information systems.

      iv. Outsourcing entities.

      v. Entities such as foreign nations and business competitors that may have an interest in information stored by DOF.

      vi. Supply chain-risks associated with high-risk systems, high-risk system components and cloud-service providers.

   b. Risk assessments must be a collaborative effort among representatives of management, operational, technology and information security disciplines.

   c. Risk assessments must use all-source intelligence to assist in the analysis of risk.

   d. Risk assessments utilize threat information provided by CSRM to determine the current cyber threat environment.

3. The System owner shall:

   a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores or transmits.

   b. The risk assessment shall be conducted as needed, but not less than once every three years.

   c. Document risk assessment results in a Risk Assessment Report, which includes, at a minimum, identification of all vulnerabilities discovered during the assessment and an executive summary, including major findings and risk mitigation recommendations.

      i. Updated reports must be sent to the CISO.

   d. Review risk assessment results at least once a year to determine the continued validity of the risk assessment.

e. Update the risk assessment once a year or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the system.

f. Use the results of the Department of Forestry BIA and of the Data Classification procedure as primary inputs to the RA.

g. Create a risk finding for any risks identified in the risk assessment with a residual risk rating greater than a value of low.

h. Create a risk treatment plan for each risk assessment finding.

4. The ISO or designee shall require DOF develop a Risk Assessment Plan.

   a. The agency head shall submit the Risk Assessment Plan to the CISO on an annual basis.

   b. The Risk Assessment Plan must include the following:

      i. The agency name, agency abbreviation and agency number.

      ii. The contact information of individual submitting the plan.

      iii. The date of submission.

      iv. The system full name and abbreviation.

      v. The planned assessor.

      vi. The date the last risk assessment was conducted for the system and

      vii. Scheduled assessment completion date.

      Note: Scheduled assessment completion date is the planned date of the completion of the future risk assessment covering a three-year period from the submission date.

5. Until completion of all corrective actions in the risk assessment, the responsible agency head or designee shall receive reports, at least quarterly, from the risk register. The quarterly risk update will report progress toward implementing outstanding risk treatments.

6. Upon completion of the risk treatments shown in the risk register, the responsible agency head or designee shall arrange for a follow-up review to verify implementation of the specified corrective actions.

7. The agency head or designee shall submit to the CISO the following information:

   a. A record of all completed IT Risk Assessments conducted by or on behalf of the agency.

   b. Agencies are required unless otherwise approved by the CISO to use the Risk Assessment Template found at: http://www.vita.virginia.gov/xxxx

   c. Each risk identified in the risk assessment template must contain:

      i. IT System Name

      ii. Risk ID

      iii. Sensitivity rating (e.g., Confidentiality, Integrity and availability)

      iv. Date of risk assessment

      v. Risk vulnerability family (e.g., SEC 501 control)

      vi. Vulnerabilities

      vii. Threats

      viii. Risk Summary

      ix. Magnitude of impact (e.g., low, moderate, high, critical)

      x. Controls in place (brief description)

d. For each risk identified, a Risk Treatment Plan must be submitted to the CISO and the plan shall include the:
   i. IT System affected
   ii. Authoritative source (e.g., SEC 501, enterprise policy, operating instruction)
   iii. Control ID (e.g., AC-1)
   iv. Date risk identified
   v. Risk summary
   vi. Risk rating (Low, Med-Low, Med, Med-High, High, Critical)
   vii. Status
   viii. Status Date
   ix. Planned resolution
   x. Resolution due date

e. The Risk Treatment Plan for completed risk assessments must be submitted within 30 days of issuing the final risk assessment report. An updated Risk Treatment Plan must be submitted quarterly (at the end of the quarter), until all resolutions are completed. All Risk Treatment Plans and quarterly updates submitted must have evidence of agency head approval.

8. The DOF director of IT is responsible for verifying and validating compliance with the provisions of this policy and procedure.

Vulnerability Monitoring and Scanning (RA-5)

1. The ISO shall require that:

   a. Information system and hosted applications must be monitored and scanned for vulnerabilities at least once every 30-days for publicly facing systems and sensitive information systems and when new vulnerabilities potentially affecting the system/applications are identified and reported.

   b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
      i. Enumerating platforms, software flaws and improper configurations.
      ii. Formatting checklists and test procedures.
      iii. Measuring vulnerability impact.

   c. Analyze vulnerability scan reports and results from vulnerability monitoring.

   d. Remediate legitimate vulnerabilities within 30 days unless otherwise specified by Commonwealth Security Risk Management in accordance with an organizational assessment of risk.

   e. Shares information obtained from the vulnerability monitoring process and control assessments with the appropriate organization-defined personnel to help eliminate similar vulnerabilities in other systems.

   f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

   g. Update the system vulnerabilities to be scanned at least once every 30 days, prior to a new scan, or when new vulnerabilities are identified and reported.

   h. The following attributes, at a minimum, are required for vulnerability testing, as required by Department of Forestry's Commonwealth Security and Risk Management, and are necessary to evaluate compliance for security certification and best practice adherence:
      i. Device Name
      ii. IP address
      iii. Device Type

iv. Wireless Access Points
v. Description
vi. OS Platform
vii. Primary Admin
viii. Location
ix. Service Type
x. Service Port
xi. Service Port Type
xii. Application
xiii. Users of Service
xiv. Network Name
xv. Network Type
xvi. Location Type
xvii. Location Access
xviii. Owning Location,
xix. User Population Name and Type
xx. Primary User contact information (e.g., phone, email).

i. Vulnerability scans must have defined a clear scope for all vulnerability scanning activities and designate knowledgeable and trained individuals to perform the scans. Prior to commencing vulnerability scanning efforts, the following should be addressed:

    i. Scanner selection – System owners shall evaluate the tools for use within their respective environments.

        1. The network and host-based vulnerability scanner must provide the following capabilities:

            a. Identify active hosts on networks.

            b. Identify active and vulnerable services (ports) on hosts.

            c. Identify vulnerabilities associated with discovered operating systems and applications.

    ii. Scope/boundaries – An active vulnerability scan must have a defined scope or boundary. The scan must be limited to a specific information system, system(s), subnet(s), or network(s) within the realm of responsibility for Department of Forestry.

        1. Scans typically should be performed only on production systems and networks that are known to be stable and preferably during times of least impact to the critical functionality of the system. It is expected that vulnerability scanning will occur during various phases of the system's life cycle.

j. Vulnerability scan reports and results from security control assessments must be analyzed.

k. Historic audit logs must be reviewed to determine if a vulnerability identified in the information system has been previously exploited.

Criticality Analysis (RA-9)

1. The ISO or designee will identify critical system components and functions by performing a criticality analysis for sensitive systems, sensitive system components or sensitive system services at least on an annual basis and following an environmental change.

Threat Hunting (RA-10)

1. The ISO or designee will:

    a. Establish and maintain a cyber threat hunting capability to:

        i. Search for indicators of compromise in organizational systems.

        ii. Detect, track and disrupt threats that evade existing controls.

    b. Employ the threat hunting capability at least on an annual basis.

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...	7/2/2024
Director of Information Technology Name (Print)	Director of Information Technology Signature	
Amanda Davis	DocuSigned by: amanda davis C2CCAD60F05A4A6...	7/9/2024
Chief of Administration Name (Print)	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