Policy and Procedure 9-19
Information Security: System and Information Integrity Policy

Issued By:	Robert W. Farrell, State Forester	DocuSigned by: Robert W. Farrell 2115C3D38FCF4E7...	7/9/2024
Effective Date:	July 8, 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 DOF 09-005 Information Security: Configuration Management Policy and Procedures		
Forms:	N/A		

CONTENTS

PURPOSE

The purpose of this policy and procedures 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: System and Information Integrity Policy and Procedure. This policy and procedure establishes the minimum requirements.

This policy and procedure is intended to meet the control requirements outlined in SEC530, Section 8.19 IT System and Information Integrity Family, controls SI-1 through SI-8, SI-10, SI-11, SI-12, SI-16, and SI-20 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.

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
SSP:	System Security Plan
VPN:	Virtual Private Network

BACKGROUND

The Information Security: System and Information Integrity Policy at Department of Forestry is intended to facilitate the effective implementation of the processes necessary to meet the IT system and communications protection requirements as stipulated by the COV ITRM Security Standard SEC530 and security best practices. This policy and procedure directs that Department of Forestry meet these requirements for all 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	System Owner	System Admin/Developer	Information Security Officer
Tasks			
Identify, report and correct information system flaws.	A	R	R
Maintain an inventory of information systems and components.	A	R	R
Test software updates.	I	R	A
Incorporate flaw remediation into configuration management process.	R		A
Monitor security sources for vulnerability announcements.	A		R
Install security-related software updates.	A	R	I
Prohibit the use of end-of-life software.			A
Employ malicious code protection mechanisms at information system entry and exit points.	I	R	A
Configure and update malicious code protection software.	A	R	R
Configure and monitor events on information systems.	A	R	R
Configure alerts for indications of compromise.	A	R	R
Install and configure intrusion detection systems.		R	A
Receive, generate, disseminate and implement security alerts, advisories, and directives.	A	R	R
Install, configure and update spam protection mechanisms.	A	R	R
Restrict the capability to input information.	A	R	R
Configure the information system to validate information inputs.	A	R	R

STATEMENT OF POLICY

In accordance with SEC530, SI-1 through SI-8, SI-10, SI-11, SI-12, SI-16, and SI-20, Department of Forestry shall develop, disseminate and periodically review/update a formal, documented, Information Security: System and Information Integrity Policy and Procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formalize documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. (SI-1)

Flaw Remediation (SI-2)

1. The information security officer (ISO) in coordination with the system owner shall identify, report and correct information system flaws.

Note: Flaws include errors in software and firmware, as well as errors in configuration settings for information systems. Flaw remediation encompasses installing software patches, service packs and malicious code signatures. Vulnerability mitigation can also involve removing software or disabling functions, ports, protocols and/or services.

2. System administrators shall test software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation.
    a. All remediation changes must be tested on non-production systems prior to implementation on all IT products and configurations in order to reduce or eliminate the following:
        i. Unintended consequences
        ii. Alteration of security settings

iii. Enabling of default user accounts that had been disabled

iv. Resetting of default passwords for user accounts

v. Enabling of services and functions that had been disabled

vi. Non-security changes, such as new functionality

b. Testing of patches must ensure that patches are installed in the required sequence and any removal of any previous security patch is not unintended.

c. Testing must include checking all related software to ensure that it is operating correctly.

d. Testing must include a selection of systems that accurately represent the configuration of the systems in deployment.

e. Based on the results of testing, it must be considered whether any significant disadvantages outweigh the benefits of installing a patch and whether remediation should be delayed until the vendor releases a newer patch that corrects the major issues.

3. The ISO shall require that:

a. Security-relevant software and firmware updates are installed within 30 days or within a timeframe approved by CSRM of the release of the updates.

b. Flaw remediation is incorporated into DOF's configuration management process.

c. System components are determined to have applicable security-relevant software and firmware updates installed using CSRM approved automated mechanisms within 30 days.

d. Measure the time between flaw identification and flaw remediation.

e. Establish the benchmark that corrective action is always taken within 30 days.

f. Employ automated patch management tools to facilitate flaw remediation to the following system components: organization-defined system components.

g. Security-relevant software and firmware updates are installed automatically to system components when possible.

h. Remove previous versions of software and firmware components after updated versions have been installed.

i. All software publisher security updates to the associated software products are applied.

4. The ISO or designee shall prohibit the use of software products that the software publisher has designated as End-of-Life/End-of-Support (i.e., software publisher no longer provides security patches for the software product).

Malicious Code Protection (SI-3)

1. The ISO or designee shall enforce the following requirements:

a. Signature or non-signature based malicious code protection mechanisms must be implemented at information system entry and exit points to detect and eradicate malicious code (e.g., firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers and mobile devices) on the network.

i. Malicious code protection mechanisms must be automatically updated as new releases are available in accordance with DOF 09-005 Information Security: Configuration Management Policy and Procedures.

ii. Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system on an organization-defined frequency and real-time scans of files from external sources at endpoint, network entry and exit points as the files are downloaded, opened or executed in accordance with organizational policy.

2. Block malicious code and send alert to administrator and ISO in response to malicious code detection.

iii. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

b. Test malicious code protection mechanisms at least on an annual basis by introducing known benign code into the system; and

i. Verify that the detection of the code and the associated incident reporting occur.

c. Employ CSRM approved tools and techniques to analyze the characteristics and behavior of malicious code.

i. Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.

d. Prohibit all IT system users from intentionally developing or experimenting with malicious programs (e.g., viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.);

e. Prohibit all IT system users from knowingly propagating malicious programs including opening attachments from unknown sources.

f. Provide malicious code protection mechanisms via multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms.

g. Provide protection against malicious program through the use of mechanisms that:

1. Eliminates, blocks or quarantines malicious programs that it detects.
2. Provides an alert notification.
3. Automatically and periodically runs scans on memory and storage devices.
4. Automatically scans all files retrieved through a network connection, modem connection, or from an input storage device.
5. Allows only authorized personnel to modify program settings.
6. Maintains a log of protection activities.

h. Provide the ability for automatic download of definition files for malicious code protection programs whenever new files become available and propagate the new files to all devices protected by the malicious code protection program.

i. Require all forms of malicious code protection to start automatically upon system boot.

j. Provide network designs that allow malicious code to be detected and removed or quarantined before it can enter and infect a production device.

k. Provide procedures that instruct administrators and IT system users on how to respond to malicious program attacks, including shut-down, restoration, notification and reporting requirements.

l. Require use of only new media (e.g., diskettes, CD-ROM) or sanitized media for making copies of software for distribution.

m. Prohibit the use of common use workstations and desktops (e.g., training rooms) to create distribution media.

n. By written policy, prohibit the installation of software on agency IT systems until the software is approved by the ISO or designee and where practicable, enforce this prohibition using automated software controls, such as active directory security policies.

o. Establish operating system (OS) update schedules commensurate with sensitivity and risk.

System Monitoring (SI-4)

1. The ISO or designee shall enforce the following requirements:

a. Events on the information system must be monitored to detect:

   i. Attacks and indicators of potential attacks in accordance with the DOF defined monitoring objectives.

   ii. Unauthorized local, network and remote connections.

b. Unauthorized use of the system must be identified through DOF defined techniques and methods.

c. Detected events and anomalies must be analyzed.

d. The level of system monitoring activity shall be adjusted when there is a change in risk to organizational operations and assts, individuals, other organizations or the Nation.

e. Legal opinion shall be obtained regarding system monitoring activities.

f. Organization defined system monitoring information provided to information security personnel as needed.

   Note: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). Information system monitoring capability is achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software and network monitoring software.

g. Connect and configure individual intrusion detection tools into an information system-wide intrusion detection system.

h. Employ automated tools and mechanisms to support near real-time analysis of events.

i. Connect and configure individual intrusion detection tools into an information system-wide intrusion detection system.

j. Employ automated tools and mechanisms to support near real-time analysis of events.

k. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic.

l. Monitor inbound and outbound communications traffic in real time for organization-defined unusual or unauthorized activities or conditions.

m. Alert information security personnel when system-generated indicators of compromise or potential compromise occurs.

n. Test intrusion-monitoring tools and mechanisms at least on an annual basis.

o. Analyze outbound communications traffic at the external interfaces to the system and selected organization-defined interior points within the system to discover anomalies.

p. Analyze communications traffic and event patterns for the system.

q. Develop profiles representing common traffic and event patterns.

r. Use the traffic and event profiles in tuning system-monitoring devices.

s. Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

t. Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.

u. Correlate information from monitoring tools and mechanisms employed throughout the system.

v. Detect network services that have not been authorized or approved by information security personnel.

w. Alert information security personnel when detected.

x. Implement the following host-based monitoring mechanisms at organization-defined system components:

i. Organization-defined host-based monitoring mechanisms.

y. Discover, collect, and distribute to information security personnel, indicators of compromise provided by Commonwealth Security and Risk Management approved sources.

Security Alerts, Advisories, and Directives (SI-5)

1. The ISO or designee shall enforce the following requirements:
   a. Information system security alerts, advisories and directives must be received from designated external organizations on an ongoing basis.
      i. All security alerts, advisories and directives must be from reputable sources (i.e., vendors, manufacturers).
   b. Internal security alerts, advisories and directives must be generated, as deemed necessary.
   c. Security alerts, advisories and directives must be disseminated to Department of Forestry personnel identified by name and/or by role.
   d. Security directives must be implemented in accordance with established time frames or the issuing organization must be notified of the degree of noncompliance.

Security and Privacy Function Verification (SI-6)

1. The ISO or designee shall enforce the following requirements:
   a. Verify the correct operation of organization-defined security and privacy functions.
   b. Perform this verification of the functions specified in SI-6a at organization-defined system transitional states, upon command by user with appropriate privilege or at least once every 90 days.
   c. Alert organization-defined personnel to failed security and privacy verification tests.
   d. Shut the system down when anomalies are discovered.
   e. Implement automated mechanisms to support the management of distributed security and privacy function testing.
   f. Report the results of security and privacy function verification to the ISO.

Software, Firmware and Information Integrity (SI-7)

2. The ISO or designee shall enforce the following requirements:
   a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware and information: organization-defined software, firmware and information.
   b. Take the following actions when unauthorized changes to the software, firmware and information are detected: notify the ISO.
   c. Perform an integrity check of organization-defined software, firmware and information at startup; at organization-defined transitional states or security-relevant events and at least once every 7 days.
   d. Employ automated tools that provide notification to the ISO upon discovering discrepancies during integrity verification.
   e. Employ centrally managed integrity verification tools.
   f. Automatically implement organization-defined controls when integrity violations are discovered.
   g. Implement cryptographic mechanisms, such as digital signatures or the application of signed hashes, to detect unauthorized changes to software, firmware and information.
   h. Incorporate the detection of the unauthorized changes into the organizational incident response capability.

i. Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions generates an audit record and alert the ISO.

j. Verify the integrity of the boot process of the following system components: organization-defined system components.

k. Implement the following mechanisms to protect the integrity of boot firmware in organization-defined system components: organization-defined mechanisms.

l. Require that the integrity of the following user-installed software be verified prior to execution: organization-defined user-installed software.

m. Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: organization-defined software or firmware components.

n. Prohibit processes from executing without supervision for more than 24 hours.

o. Implement organization-defined controls for application self-protection at runtime.

Spam Protection (SI-8)

1. The ISO or designee shall enforce the following requirements:

   a. Spam protection mechanisms must be employed at information systems entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers or mobile computing devices on the network.

   b. Spam protection mechanisms must be used to detect and act on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses or other common means.

   c. Spam protection mechanisms (including signature definitions) must be updated when new releases are available.

   d. Spam protection mechanisms should be updated automatically on a daily basis.

   e. Spam protection mechanisms with a learning capability should be implemented to identify legitimate communications traffic more effectively.

Information Input Validation (SI-10)

1. The ISO or designee shall enforce the following requirements:

   a. The information system must be configured to check the validity of information inputs.

      i. The checks for input validation must be verified as part of system testing.

   b. The information system must be configured to check all arguments or input data strings submitted by users, external processes or untrusted internal processes.

      i. The information system must validate all values that originate externally to the application program itself, including arguments, environment variables and information system parameters.

   c. Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) must be in place to verify that inputs match specified definitions for format and content.

   d. The information system must be configured to perform the following input validations:

      i. Type checks – Checks to ensure that the input is, in fact, a valid data string and not any other type of object.

         1. This includes validating that input strings contain no inserted executable content or active content that can be mistakenly interpreted as instructions to the system, including, but not limited to; trojan horses, malicious code, metacode, metadata or metacharacters, Hypertext Markup Language (HTML), Extensible Markup Language (XML), JavaScript, Structured Query Language (SQL) statements, shell script and streaming media.

2. Inputs passed to interpreters must be prescreened to prevent the content from being unintentionally interpreted as commands.

ii. Format and syntax checks – Checks to verify that data strings conform to defined formatting and syntax requirements for that type of input.

iii. Parameter and character validity checks – Checks to verify that any parameters or other characters entered, including format parameters for routines that have formatting capabilities, have recognized valid values.

1. Any parameters that have invalid values must be rejected and discarded.

2. Web server applications must be configured to prohibit invalid data from web clients in order to mitigate web application vulnerabilities including, but not limited to, buffer overflow, cross-site scripting, null byte attacks, SQL injection attacks, and HTTP header manipulation.

e. Input validation errors must be reviewed and resolved at least within 30 days of discovery.

f. The system must behave in a predictable and documented manner when invalid inputs are received.

g. The system must prevent untrusted data injections.

h. Invalid inputs or error statements must not give the user sensitive data, storage locations, database names, or information about the application or information system's architecture.

Error Handling (SI-11)

1. The ISO or designee shall enforce the following requirements:

a. Information systems must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

b. Error messages should be revealed only to the ISO and appropriate organization-defined personnel.

Information Management and Retention (SI-12)

1. The ISO or designee shall enforce the following requirements:

a. Information systems must manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guideline, and operational requirements.

b. Techniques to minimize the use of personally identifiable information for research, testing or training may include obfuscation hashing or other DOF defined technique.

c. Reduce security and privacy risks by disposing of information when it is no longer needed in accordance with SEC 514; disposal applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information.

Memory Protection (SI-16)

1. The ISO or designee shall enforce the following requirements:

a. Malicious code protection and other DOF defined controls must be implemented to protect the system memory from unauthorized code execution.

Tainting (SI-20)

1. The ISO or designee shall enforce the following requirement:

a. Embedded data or capabilities DOF specific systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization.

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...	7/8/2024
Director of Information Technology Name (Print)	Director of Information Technology Signature	
Amanda Davis	DocuSigned by: amanda davis C2CCAB60F85A4A6...	7/9/2024
Chief of Administration Name (Print)	Chief of Administration Signature	

VERSION HISTORY

Version History			
Date	**Version**	**Details**	**Author/Contributors**
July 8, 2024	1	Original – CSRM template and updated with SEC530	Catherine Shefski, ISO