Policy and Procedure 9-18
Information Security: System and Communications Protection 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		
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 IT System and Communications Protection Policy. This policy and procedure establishes the minimum requirements.

This policy is intended to meet the control requirements outlined in SEC530, Section 8.18 IT System and Communications Protection Family, controls SC-1 through SC-50 as well as additional Commonwealth of Virginia controls.

SCOPE

All Department of Forestry employees (classified, hourly, or business partners) as well as all sensitive 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
DMZ:	Demilitarized Zone
DOF:	Department of Forestry
IDS:	Intrusion Detection System
IPS:	Intrusion Prevention System
ISO:	Information Security Officer
IT:	Information Technology
ITRM:	Information Technology Resource Management
SEC530:	Information Security Standard 530
VPN:	Virtual Private Network

BACKGROUND

The Information Security: System and Communications Protection Policy and Procedure 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 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	**Data Owner**	**System Owner**	**System Admin/Developer**	**Information Security Officer**
Tasks				
Design and configure information system to separate user functionality from management functionality		A	R	R
Configure information system to isolate security functions from non-security functions		A	R	R
Configure information system to maintain a separate execution domain		A	R	R
Configure information system to prevent unauthorized and unintended information transfer via shared system resources		A	R	R
Configure information system to monitor and control communications		A	R	R
Protect the integrity and availability of publicly available information and applications.	A		R	R
Inventory publicly available servers			R	A
Log and save audit trails on sensitive systems	A		R	R
Perform security audits	A			R
Provide data origin and integrity artifacts with authoritative data.		A	R	R

STATEMENT OF POLICY

In accordance with SEC530, SC-1 through SC-50, DOF shall establish minimum requirements for the protection of systems and communications. The ISO is designated to manage the development, documentation and dissemination of the Information Security: System and Communications Protection policy and procedures which will be reviewed and updated annually and following an environmental change. (SC-1)

Application Partitioning (SC-2)

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

   a. The information system must be designed and configured to separate user functionality (including user interface services) from system management functionality (e.g., functions necessary to administer databases, network components, workstations or servers, and typically requires privileged user access).

Note: An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.

   b. The information system must be designed and configured to either physically or logically separate user functionality from information system management functionality.

i. Separation must be accomplished by using one of the following methods or a combination of methods, as applicable:

1. Different computers
2. Different partitions
3. Different central processing units
4. Different instances of the operating system
5. Different network addresses
6. Employing virtualization techniques
7. Other methods as appropriate

ii. Store applications and software separately from state information about users' interactions with and application to better protect individuals' privacy.

Security Function Isolation (SC-3)

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

a. The information system must be configured to isolate security functions from non-security functions by means of isolation boundaries (implemented via partitions and domains) that control access to and protect the integrity of the hardware, software and firmware that perform those security functions.

Information in Shared System Resources (SC-4)

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

Note: The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

a. The information system must be configured to prevent unauthorized and unintended information transfer via shared system resources.

Note: The control of information in shared resources is also referred to as object reuse.

Denial of Service Protection (SC-5)

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

a. The information system must be configured to:

i. Protect against or limit the effects of the following types of denial-of-service events: resource exhaustion, amplification attack and organization-defined types of denial-of-service events.

ii. Employ the following controls to achieve the denial-of-service objective: application firewall and additional organization-defined controls by type of denial-of-service events.

iii. Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: all denial-of-service attacks except for system testing purposes.

iv. Manage capacity, bandwidth or other redundancy to limit the effects of information flooding denial-of-service attacks.

v. Employ the following monitoring tools to detect indicators of denial-of-service attacks against or launched from, the system: intrusion detection and application firewall.

vi. Monitor the following system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks: organization-defined system resources.

Resource Availability (SC-6)

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

a. The information system must be configured to:

i. Protect the availability of resources by allocating organization-defined resources by priority.

Boundary Protection (SC-7)

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

a. The information system must be configured to:

i. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system.

ii. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks.

iii. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

iv. Limit the number of external connections to the system.

b. DOF shall consider the intrinsically shared nature of external telecommunications services in the implementation of security controls associated with the use of such services.

i. When external telecommunications services are employed, the following must be complied with:

a. Implement a managed interface for each external telecommunication service.

b. Establish a traffic flow policy for each managed interface.

c. Protect the confidentiality and integrity of the information being transmitted across each interface.

d. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need.

e. Review exceptions to the traffic flow policy at least on an annual basis and following an environmental change and remove exceptions that are no longer supported by an explicit mission or business need.

f. Prevent unauthorized exchange of control plane traffic with external networks.

g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks.

h. Filter unauthorized control plane traffic from external networks.

c. Boundary/edge devices (e.g., firewalls, routers) must be configured to protect and control access to DOF information resources including:

i. Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces.

ii. Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using a Commonwealth Security and Risk Management approved solution.

iii. Route organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers at managed interfaces.

iv. Detect and deny outgoing communications traffic posing a threat to external systems.

v. Audit the identity of internal users associated with denied communications.

vi. Only allows incoming communications from organization-defined authorized sources to be routed to organization-defined authorized destinations.

vii. Implement organization-defined host-based boundary protection mechanisms at the appropriate organization-defined information system component layer.

viii. Isolate organization-defined information security tools, mechanisms and support components from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

ix. Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

x. Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

xi. Block inbound and outbound communications traffic between organization- defined communication clients that are independently configured by end users and external service providers.

xii. Prohibit the direct connection of organization-defined system to a public network.

xiii. Implement logically separate subnetworks to isolate the following critical system components and functions: organization-defined critical system components and functions.

Transmission Confidentiality and Integrity (SC-8)

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

Note: This control applies to communications across internal and external networks.

a. The information system must be configured to protect the confidentiality and integrity of transmitted information.

b. If commodity commercial transmission services rather than a fully dedicated transmission service are used and it is infeasible or impractical to obtain from the service provider the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, then one or both of the following must be complied with:

i. Appropriate compensating security controls must be implemented.

ii. The additional risk must be explicitly accepted.

c. Cryptographic mechanisms must be employed to prevent unauthorized disclosure of information and to detect changes to information during transmission and can include:

i. TLS

ii. IPSec

iii. Hash functions

iv. Checksums

v. Message authentication codes

d. Data protection mechanisms must be used for the transmission of all email and attached data that is sensitive. Relative to integrity.

e. Encryption must be used for the transmission of email and attached data that is sensitive relative to confidentiality. The ISO should plan for the issue of agency email being intercepted, incorrectly addressed or infected with a virus.

Network Disconnect (SC-10)

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

a. Network connection associated with a communications session must be terminated at the end of the session or after 15 minutes of inactivity.

Cryptographic Key Establishment and Management (SC-12)

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

a. Cryptographic keys must be established and managed by using manual procedures or automated mechanisms with supporting manual procedures when cryptographic protection is required and the information system is not covered by an enterprise solution.

   i. A fully automated key management system is preferred to eliminate or reduce the opportunity for an individual to expose a key or influence the key creation.

   ii. The secure key management system will be used for the administration and distribution of encryption keys.

b. Availability of information must be maintained in the event of the loss of cryptographic keys by users.

c. Produce, control and distribute symmetric cryptographic keys using NIST FIPS 140-3 validated key management technology and processes.

d. Produce, control and distribute asymmetric cryptographic keys using certificates issued in accordance with organization-defined requirements.

e. Define the process for the creation and storage of any cryptographic keying material used to protect organization-defined information rated sensitive for confidential or integrity agency practices for selecting and deploying encryption technologies and for the encryption of data.

f. Document the procedure for the creation and storage of any cryptographic keying material used to protect organization-defined information rated sensitive for confidential or integrity.

Use of Cryptography (SC-13)

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

   a. The information system must implement required cryptographic protections using cryptographic modules that comply with applicable laws, directives, policies, regulations, standards and guidance.

      i. All sensitive data must be encrypted with a validated technology solution such as FIPS-validated cryptography or NSA-approved cryptography.

   b. Agency practices must be defined and documented for selecting and deploying encryption technologies and for the encryption of data.

   c. Before implementing encryption, appropriate processes must be documented. These processes must include the following components:

      i. Instructions in the IT Security Agency's Incident Response Plan on how to respond when encryption keys are compromised.

      ii. A secure key management system for the administration and distribution of encryption keys.

      iii. Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss due to unexpected circumstances.

   d. Encryption must be employed for the transmission of data that is sensitive relative to confidentiality or integrity over non-Commonwealth networks or any publicly accessible networks or any transmission outside of the data's broadcast domain. Digital signatures may be utilized for data that is sensitive solely relative to integrity.

Collaborative Computing Devices and Applications (SC-15)

1. The ISO or designee shall enforce the following requirements for collaborative computing devices and applications:

NOTE: Collaborative computing devices and applications include remote meeting devices and applications, networked white boards, cameras and microphones.

   a. Remote activation of collaborative computing devices and applications are prohibited with the following exception:

i. Computer support that a user explicitly approves.

b. When collaborative computing devices and applications are in use, an explicit indication of use to users physically present must be given.

c. Provide easy methods, manual or automatic, to disconnect from collaborative devices or applications, physical or logical, to ensure participants can disconnect easily, preventing subsequent compromises of organizational information.

d. Provide an explicit indication of current participants in all online meetings and teleconferences.

Public Key Infrastructure Certificates (SC-17)

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

a. Public key certificates must be issued under a DOF-defined certificate policy or obtained under an appropriate certificate policy from an approved service provider.

b. Only approved trust anchors in trust stores or certificate stores managed by the organization will be included.

Mobile Code (SC-18)

1. The ISO or designee shall:

a. Define acceptable and unacceptable mobile code and mobile code technologies.

b. Authorize, monitor and control the use of mobile codes within the system.

Secure Name/Address Resolution Service (Authoritative Source) (SC-20)

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

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

c. Provide data origin and integrity protection artifacts for internal name/address resolution queries.

Secure Name/Address Resolution Service (Recursive or Caching Resolver) (SC-21)

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

a. The information systems must request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Architecture And Provisioning for Name/Address Resolution Service (SC-22)

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

a. The information system must ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

Session Authenticity (SC-23)

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

a. The information system must provide mechanisms to protect the authenticity of communications sessions.

i. A unique session identifier for each session must be generated with randomness and recognize only session identifiers that are system-generated.

ii. Only the use of approved certificate authorities is allowed for verification of the establishment of protected sessions.

Note: This control focuses on communications protection at the session not the packet level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example: this control addresses man-in-the- middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).

2. The system owner shall select and implement protection mechanisms to ensure adequate protection of data integrity, confidentiality and session authenticity in transmission.

   a. Mechanisms include but are not limited to the following:

      i. Security services based on IPsec

      ii. VPNs

      iii. TLS

      iv. DNS

      v. SSH

      vi. SSL

      vii. Digital signatures

      viii. Digital certificates

      ix. Digital time stamping

      x. Approved encryption requirements and technology:

         1. FIPS 140-2

         2. Use of AES 128 bit or higher

Protection of Information at Rest (SC-28)

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

Note: This control is intended to address the confidentiality and integrity of information at rest in non-mobile devices and covers user information and system information.

   a. The information system must protect the confidentiality and integrity of sensitive information at rest (i.e., the state of information when it is located on a secondary storage device within an information system).

      i. User and system information at rest in non-mobile devices must be protected.

   b. The storage of sensitive data on any non-network storage device, excluding backup media, must be encrypted. A written exception approved by the agency head or his/her designee must be in place prior to storing encrypted sensitive data on non-network storage devices.

      i. Non-network storage devices include removable data storage media and the fixed disk drives of all desktops and mobile workstations, such as laptop and tablet computers, USB drives, CDs, etc.

   c. Sensitive data at rest must be encrypted when mandated by federal, state or local laws as well as industry regulations, (e.g., IRS1075, HIPAA and PCI.)

Out of Band Channels (SC-37)

DOF does not use out of band channels.

Sensor Capability and Data (SC-42)

1. The ISO or designee shall enforce the following for systems or system components with sensor capability and data, such as mobile devices, cellphones or tablets with GPS mechanisms and accelerometers:
    a. Prohibit the remote activation of environmental sensing capabilities on organizational systems or system components with the following exception: agency head approved policy, indicating business functions that cannot be accomplished without the use of the capability.
    b. Provide an explicit indication of sensor use to the user of the device.
    c. Verify that the system is configured so that data or information collected by the organization-defined sensors is only reported to authorized individuals or roles.
    d. Provide training to authorized collectors of any DOF data to ensure information collected is only used for authorized purposes.
    e. Exceptions to remote activation of environmental capabilities are permitted if required as part of an authorized incident response activity and only provides an indication of the sensor use if authorized by the incident response team.

Usage Restrictions (SC-43)

1. The ISO or designee shall:
    a. Establish usage restrictions and implementation guidance for the following system components: as defined in SEC528.
        i. All system components including, but not limited to:
            1. Mobile code
            2. Mobile devices
            3. Wireless access
            4. Wired and wireless peripheral components (copiers, scanners, optical devices, etc.)
    b. Authorize, monitor and control the use of such components within the system.

Detonation Chambers (SC-44)

1. The ISO or designee shall employ a detonation chamber, or dynamic execution environments, capability within systems supporting incident response activities.

Note: Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications and execute Universal Resource Locator requests in the safety of an isolated environment or a virtualized sandbox. Protected and isolated execution environments provide a means of determining whether the associated attachments or applications contain malicious code.

System Time Synchronization (SC-45)

1. The ISO or designee shall require:
    a. Synchronize system clocks within and between systems and system components such that:
        i. Compare the internal system clocks at least every 1024 seconds with Commonwealth approved time servers.
        ii. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than 100 milliseconds.
        iii. Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source.

iv. Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable.

Cross Domain Policy Enforcement (SC-46)

1. The ISO or designee shall implement a policy enforcement mechanism logically between the physical and/or network interfaces for the connecting security domains.

Alternate Communication Paths (SC-47)

1. The ISO or designee shall establish organization-defined alternate communications paths for system operations organizational command and control.

Software-Enforced Separation and Policy Enforcement (SC-50)

1. The ISO or designee shall implement software-enforced separation and policy enforcement mechanisms between organization-defined security domains.

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...
7/8/2024
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
July 8, 2024	1	Original – CSRM template and updated with SEC530	Catherine Shefski, ISO