Policy and Procedure 9-9
Information Security: System Maintenance

Issued By:	Robert W. Farrell, State Forester	DocuSigned by: Robert W. Farrell 2115C3D38FCF4E7...	7/1/2024
Effective Date:	June 10, 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 1
SCOPE 1
DEFINITIONS and ACRONYMS 1
BACKGROUND 2
ROLES & RESPONSIBILITY 2
STATEMENT OF POLICY 3
- Controlled Maintenance (MA-2) 3
- Maintenance Tools (MA-3) 3
- Nonlocal Maintenance (MA-4) 4
- Maintenance Personnel (MA-5) 4
- Timely Maintenance (MA-6) 5

AUTHORITY 5
INTERPRETATION 5
APPROVAL 5
Version History 6

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: System Maintenance Policy and Procedure. This policy and procedure establishes the minimum requirements for system maintenance.

This policy is intended to meet the control requirements outlined in SEC530, Section 8.9 System Maintenance Family, Controls MA-1 through MA-6.

SCOPE

All Department of Forestry employees (classified, hourly, or business partners) as well as all 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 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
DOF:	Department of Forestry
DRP:	Disaster Recovery Plan
ISO:	Information Security Officer
IT:	Information Technology
ITRM:	Information Technology Resource Management
SEC530:	Information Security Standard 530
VCCC:	VITA Customer Care Center
VITA	Virginia Information Technology Agency

BACKGROUND

The Information Security System Maintenance Policy and Procedure is intended to facilitate the effective implementation of the processes necessary to meet the system maintenance requirements as stipulated by the COV ITRM Security Standard SEC530 and security best practices. This policy and procedure directs that DOF meet these requirements.

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	Information Security Officer
Tasks				
Schedule, perform, document, and review records on maintenance		A	R	R
Control all maintenance activities		A	R	R
Sanitize equipment prior to offsite maintenance		A	R	R
Checks security controls following maintenance		A	R	R
Maintain system maintenance records		A	R	R

Ensure that personnel performing maintenance on the information system have required access authorizations		A	R	R

STATEMENT OF POLICY

In accordance with SEC530, Department of Forestry shall ensure all maintenance, diagnostic and repair activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location, are managed and monitored to preserve the confidentiality, integrity and availability of Department of Forestry's information systems.

Controlled Maintenance (MA-2)

1. The ISO or designee shall:
    a. Schedule, perform, document and review records of maintenance, repair and replacement on information system components in accordance with manufacturer or vendor specifications and Department of Forestry requirements.
    b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location.
    c. Explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance, repairs or replacement.
    d. Sanitize equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance, repair or replacement.
    e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair action.
    f. Include information system maintenance records for the life of the system that include:
        i. Date and time of maintenance.
        ii. Name(s) of the individual(s) performing the maintenance.
        iii. Name of escort (if necessary).
        iv. Description of maintenance performed.
        v. List of equipment removed or replaced (including identification numbers if applicable).

Maintenance Tools (MA-3)

1. The ISO or designee shall:
    a. Approve, control, and monitor the use of system maintenance tools and review previously approved system maintenance tools annually to include.
        i. Inspection of maintenance tools used by maintenance personnel for improper or unauthorized modifications.
        ii. Check media containing diagnostic and test programs for malicious code before the media are used in the system.
        iii. Prevent the removal of maintenance equipment containing organizational information by:
            1. Verifying that there is no organizational information contained on the equipment.
            2. Sanitizing or destroying the equipment.
            3. Retaining the equipment within the facility.
            4. Obtaining an exemption from ISO or designee explicitly authorizing removal of the equipment from the facility.

iv. Restrict the use of maintenance tools to authorized personnel only.

v. Monitor the use of maintenance tools that execute with increased privilege.

vi. Inspect maintenance tools to ensure the latest software updates and patches are installed.

Nonlocal Maintenance (MA-4)

1. The ISO or designee shall:
   a. Approve and monitor nonlocal maintenance and diagnostic activities.
   b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system.
   c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.
   d. Maintain records for nonlocal maintenance and diagnostic activities.
   e. Terminate session and network connections when nonlocal maintenance is completed.
   f. Log organization-define audit events for nonlocal maintenance and diagnostic sessions.
   g. Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.
   h. Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced or
   i. Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitizes the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.
   j. Protect nonlocal maintenance sessions by:
      i. Employing organization-defined authenticators that are replay resistant.
      ii. Separating the maintenance sessions from other network sessions with the system by either:
         1. Physically separated communications paths; or
         2. Logically separated communications paths.
   k. Require the approval of each nonlocal maintenance session by organization-defined personnel.
   l. Notify the following personnel or roles of the date and time of planned nonlocal maintenance: organization-defined personnel or roles.
   m. Implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: organization-defined cryptographic mechanisms.
   n. Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.

Maintenance Personnel (MA-5)

1. The ISO or designee shall ensure that personnel performing maintenance on the information system have required access authorizations or designate organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.
   a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.
   b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations.

c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

d. Third-party maintenance providers under contract to perform maintenance/support services on DOF information systems shall provide a list of field service engineers assigned to support DOF maintenance contract with the following information for each service representative:

   i. Name

   ii. Company represented

   iii. Title

   iv. Contact Info (phone number; e-mail)

   v. Photo for identification purposes

   vi. List of systems individual is authorized to perform maintenance on

   vii. The organization shall develop and publish a maintenance personnel policy that requires all system/service maintenance and support be performed by United States citizens, residents, or individuals with a valid H1B visa.

Timely Maintenance (MA-6)

1. The ISO or designee shall:

   a. Obtain maintenance support and/or spare parts for organization-defined business-critical information system components to resolve issues within the acceptable organization-defined time period of failure.

   b. Perform preventive maintenance on organization-defined information system components at the appropriate organization-defined time intervals to ensure that the business need is met.

   c. Perform predictive maintenance on information system components at least on an annual basis and following an environmental change.

   d. Transfer predictive maintenance data to a maintenance management system using organization-defined automated mechanisms.

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...	6/11/2024
Director of Information Technology Name (Print)	Director of Information Technology Signature	
Amanda Davis	DocuSigned by: amanda davis C2CCAB60F85A4A6...	6/27/2024
Chief of Administration Name (Print)	Chief of Administration Signature	

Version History

Version History			
Date	**Version**	**Details**	**Author/Contributors**
June 10, 2024	1	Original – CSRM template and updated with SEC530	Catherine Shefski, ISO