Policy and Procedure 9-10
Information Security: Media Protection

Issued By:	Robert W. Farrell, State Forester	DocuSigned by: Robert W. Farrell 2115C3D38FCF4E7...	6/24/2024
Effective Date:	June 11, 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: Media Protection Policy and Procedure. This policy and procedure establishes the minimum requirements for the Information Security: Media Protection Policy and Procedure.

This policy is intended to meet the control requirements outlined in SEC530, Section 8.10 Media Protection Family, Controls MP-1 through MP-7, 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 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.

"VITA" means the Virginia Information Technology Agency

ACRONYMS

CIO:	Chief Information Officer
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
SEC530:	Information Security Standard 530
VITA	Virginia Information Technology Agency

BACKGROUND

The Information Security: Media Protection Policy and Procedure is intended to facilitate the effective implementation of the processes necessary to meet the media protection requirements as stipulated by the COV ITRM Security Standard SEC530 and security best practices. This policy and procedure directs the 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	Data Owner	System Owner	System Admin	Information Security Officer
Tasks				
Document and implement data storage media protection practices.	I			A/R
Define protection of stored sensitive data.	A			C
Prohibit the storage of sensitive data on any non-network storage device or media.	R		R	A
Prohibit the storage of any commonwealth data on IT systems that are not under contractual control of the commonwealth.	R		R	A

Prohibit the connection of any non-COV owned or leased data storage media or device to a COV-owned or leased device.	R	R	R	A
Prohibit the auto forwarding of emails to external accounts.	R		R	A
Document policies and procedures for the media requiring restricted access.		A		R
Implement and document procedures to safeguard handling of all backup media.	A			R
Document activities associated with the transport of information system media.		R		A
Employ an identified custodian throughout the transport of information system media.		A		I
Require that information system media is sanitized prior to disposal, release or reuse.	A		R	I
Track, document and verify media sanitation and disposal actions.	A		R	I
Follow sanitation procedures.	A		R	I

STATEMENT OF POLICY

In accordance with SEC530, MP-1 through MP-7, DOF will document policies and procedures to define the course of action to prevent unauthorized use or misuse of Commonwealth data and promote the privacy and security of sensitive information within DOF and its customers. This policy will be overseen by the ISO and be reviewed annually and following any environmental change.

Policy and Procedures (MP-1)

1. The ISO or designee shall document and implement Data Storage Media protection practices. At a minimum, these practices must include the following components:

   a. Define protection of stored sensitive data as the responsibility of data owner.

   b. Prohibit the storage of sensitive data on any non-network storage device or media, except for backup media, unless the data is encrypted and there is a written exception approved by the agency head accepting all residual risks (Note: This type of exception is an agency level exception only and does not need to be approved by Commonwealth Security).

      i. The exception shall include the following elements:

         1. The business or technical justification.

         2. The scope, including quantification and duration (not to exceed one year).

         3. A description of all associated risks.

         4. Identification of controls to mitigate the risks, one of which must be encryption.

         5. Identification of any residual risks.

   c. Prohibit the storage of any Commonwealth data on IT systems that are not under the contractual control of the Commonwealth of Virginia. The owner of the IT system must adhere to the latest Commonwealth of Virginia information security policies and standards as well as the latest Commonwealth of Virginia auditing policies and standards.

   d. Prohibit the connection of any non-COV owned or leased data storage media or device to a COV-owned or leased resource, unless connecting to a guest network or guest resources. This prohibition, at the agency's discretion need not apply to an approved vendor providing operational IT support services under contract.

      i. DOF employees are allowed to bring personal IT assets onto DOF or business partner premises that house COV IT systems and data although personal IT assets may not be connected to the DOF or business partner network.

   e. Prohibit the auto forwarding of emails to external accounts to prevent data leakage unless there is a documented business case disclosing residual risk approved in writing by the agency head.

Media Access (MP-2)

1. The ISO shall require that access to digital and non-digital media is restricted to authorized individuals only, using organization-defined security measures.

- **Note:** Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras and audio recording devices).

2. Assessment of risk must guide the selection of media and associated information contained on that media requiring restricted access.
3. System owners must document policies and procedures for the media requiring restricted access, individuals authorized to access the media and the specific measures taken to restrict access.

Media Marking (MP-3)

Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), flash drives, compact discs and digital versatile discs. Non-digital media includes paper and microfilm. Controlled unclassified information is defined by the National Archives and Records Administration along with the appropriate safeguarding and dissemination requirements for such information and is codified in [32 CFR 2002]. Security markings are generally not required for media that contains information determined by organizations to be in the public domain or to be publicly releasable. System media marking reflects applicable laws, executive orders, directives, policies, regulations, standards and guidelines.

1. The ISO shall require:
   a. Mark system media indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information.

   b. Exempt organization-defined types of system media from marking if the media remain within organization-defined controlled areas.

Media Storage (MP-4)

1. The ISO or designee shall implement and document procedures to safeguard handling of all backup media containing sensitive data. At a minimum, these procedures must include the following requirements:
   a. Physically controlling and securely storing digital and non-digital media within organization-defined controlled areas using organization-defined security measures.

   b. Protecting information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Media Transport (MP-5)

1. The ISO requires that:
   a. All digital and non-digital media is protected and controlled during transport outside of controlled areas using FIPS 140-2 validated encryption module for all digital media and a secured locked container for non-digital media.

      i. DOF employees are responsible for safeguarding any IT assets they remove from DOF or business partner premises, including keeping these assets under their direct physical control whenever possible, and physically securing the assets (i.e., by means of lock and key) when they are not under the employee’s direct physical control.

   b. Accountability for information system media is maintained during transport outside of controlled areas.

      i. DOF employees must immediately report loss or theft of any IT assets assigned to them to their supervisor and to the ISO.

c. Activities associated with transport of such media are restricted to authorized personnel.

i. DOF employees shall not remove DOF or business partner owned IT assets from agency or company premises.

1. One exception to this policy is IT assets assigned to employees to include laptop computers, cellular telephones, and Personal Digital Assistant (PDA) devices.

2. The ISO or designee shall document, using established documentation requirements, activities associated with the transport of information system media in accordance with the organizational assessment of risk to include the flexibility to define different record-keeping methods for different types of media transport as part of an overall system of transport-related records.

a. At a minimum, any log or tracking mechanism must include:

i. Description of information being transported.

ii. Type of information (e.g., PII) contained on the media.

iii. Method(s) of transport.

iv. Protection measures employed.

v. Name(s) of individual(s) transporting the information (if appropriate).

vi. Authorized recipient(s).

vii. Dates sent and received.

b. Before transporting, delivering or mailing media containing sensitive information, individuals shall:

i. Notify the entity authorized to receive the information.

ii. Document the following information:

1. An identifying document number, if used.

2. Description of the information.

3. Name and signature of the sender.

4. Date sent.

c. Media containing sensitive information transported by a common carrier must use an acknowledgement of receipt.

d. Personnel transporting sensitive information by car shall store the media in a locked trunk while en route.

i. If a trunk is not available in the vehicle, the media must be hidden from sight.

ii. Personnel are prohibited from leaving media containing sensitive information in a vehicle overnight.

iii. If media containing sensitive information is being transported and delivered by hand, then it must be given directly to the recipient or another authorized individual.

3. The system owner shall employ an identified custodian throughout the transport of sensitive information system media.

a. Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

Media Sanitization (MP-6)

1. The ISO requires that information system media, both digital and non-digital, is sanitized prior to disposal, release out of organizational control or release for reuse.

a. Media sanitization and disposal actions must be tracked, documented and verified.

b. Sanitization equipment and procedures must be tested to verify correct performance in accordance with the current version of the Removal of Commonwealth Data from Electronic Media Standard (COV ITRM Standard SEC514).

c. Sanitization of portable, removable storage devices must be completed prior to connecting such devices to the information system.

d. Sanitization of portable, removable storage devices, must be considered when:

   i. Such devices are first purchased from the manufacturer or vendor prior to initial use or

   ii. When the organization loses a positive chain of custody for the device.

e. An assessment of risk must guide the specific circumstances for employing the sanitization process.

f. Information system media must be destroyed that cannot be sanitized.

g. Removal of data from IT assets must be completed prior to disposal in accordance with the current version of the Removal of Commonwealth Data from Electronic Media Standard (COV ITRM Standard SEC514).

   i. Data owners of data residing on DOF owned or leased hard drives and electronic media will perform, or cause to be performed, the following procedures:

      1. Before the removal process begins, the computer must be disconnected from any network to prevent accidental damage to the network operating system or other files on the network.

      2. The method used for removal of DOF and customer data, depends upon the operability of the hard drive and or electronic media.

      3. Whenever licensed software is resident on any electronic media being surplused, transferred, traded-in, disposed of, or replaced, the terms of the license agreement shall be followed.

      4. Operable hard drives and or electronic media that will be reused must be overwritten prior to disposition. If the hard drive and or electronic media is removed, is inoperable or has reached the end of its useful life, it must be physically destroyed or degaussed.

      5. Deleting files or using the format command does not prevent data from being recovered by technical means and therefore it is not an acceptable method of removing data from agency owned or leased hard disk storage media.

      6. Electronic media shall be securely erased at the earliest time after being taken out of use but not later than 60 days.

2. One of the following three acceptable methods shall be used for the removal of data from hard drives:

   a. Overwriting – Overwriting is an approved method for removal of Commonwealth data from hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented. The overwriting process including the software products and applications used for the overwriting process shall include the following steps:

      i. The data shall be properly overwritten with pseudo random data by means of, at a minimum, one pass of the entire device for a 15 gigabyte or greater drive. A minimum of three passes of pseudo random data must be applied to drives smaller than 15 gigabytes in size.

      ii. The software shall have the capability to overwrite the entire hard disk drive, independent of any BIOS or firmware capacity limitation that the system may have, making it impossible to recover any meaningful data.

      iii. The software shall have the capability to overwrite using a minimum of one pass or three passes of pseudo random data on all sectors, blocks, tracks and any unused disk space on the entire disk medium.

      iv. The software or supporting software shall have a method to verify that all data has been removed. Verification must be performed to verify that each drive overwritten is, in fact, clean of any intelligible or prior data. This verification can be either as a separate process or included as part of the software used for overwriting.

v. Sectors not overwritten shall be identified and if they cannot be removed overwriting is not acceptable and another method must be employed.

b. Degaussing – A process whereby the magnetic media are erased, (i.e., returned to a zero state). Degaussing (demagnetizing) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable by keyboard or laboratory attack.

i. Hard drives and or electronic media cannot be used after degaussing. The degaussing method will only be used when the hard drive and or electronic media is inoperable and will not be used for further service.

- **Note:** Extreme care should be used when using degaussers since this equipment can cause extreme damage to nearby telephones, monitors, and other electronic equipment. Also, the use of a degausser does not guarantee that all data on the hard drive will be destroyed. Degaussing efforts will be audited periodically to detect equipment or procedure failures.

c. Physical Destruction – Hard drives should be physically destroyed when they are defective or cannot be economically repaired or Commonwealth data cannot be removed for reuse. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive.

i. Hard drives shall be destroyed when they are defective or cannot be repaired or DOF or customer data cannot be removed for reuse.

ii. Physical destruction shall be accomplished to an extent that precludes any possible further use of the hard drive. This can be attained by removing the hard drive from the cabinet and removing any steel shielding materials and/or mounting brackets and cutting the electrical connection to the hard drive unit.

iii. The hard drive should then be subjected to physical force (pounding with a sledgehammer) or extreme temperatures (incineration) that will disfigure, bend, mangle or otherwise mutilate the hard drive so it cannot be reinserted into a functioning computer.

iv. Multiple holes drilled into the hard disk platters is an optional method of destruction that will preclude use of the hard drive and provide reasonable protection of data written on the drive.

3. Electronic devices that hold user data or configurations in non-volatile memory shall have all DOF or customer data removed by either the removal of the battery or electricity supporting the non-volatile memory or by such other method recommended by the manufacturer for devices where the battery is not removable. This is to include all computer equipment that has memory such as personal computers, PDAs, routers, firewalls and switches.

4. If there is any risk of disclosure of sensitive data on media other than hard drives or devices that hold user data or configurations in non-volatile memory, that media should be overwritten, degaussed or destroyed. Disintegration, incineration, pulverization, shredding or melting are acceptable means of destruction. Examples of other media include, but are not limited to, tapes, diskettes, CDs, DVDs, worm devices and USB data storage devices.

5. DOF or customer will audit the removal of data for compliance with this policy and procedure when any computer hard drives or electronic media are made surplus, transferred, traded-in, disposed of, or the hard drive is being replaced to ensure the audit process occurs in a timely manner and the audit controls are effective.

a. The removal of Commonwealth data must be performed and documented as required in the COV ITRM Standard (SEC514).

b. The certification form must be completed and a copy affixed to the hard drive as required in the COV ITRM Standard (SEC514).

6. Recommended software for the removal of commonwealth data from hard drives and electronic media is covered in the COV ITRM Standard (SEC514).

7. If recovery of data contained on an electronic storage media is required, DOF or its service provider must provide adequate controls commensurate with the sensitivity of the data contained on the storage media as follows:

a. If a third party is used to recover the data, the agency must ensure that the work is performed in accordance with the requirements for data protection as outlined in the COV IT Security Policy and Standard.

b. Department of Forestry may require a non-disclosure agreement and/or confidentiality agreement in order to strictly enforce the privacy of the data.

c. If the media must be removed from DOF or customer premises and sent offsite for recovery, DOF must ensure that the vendor provides a secure facility and safeguarding capabilities such as background checks, etc. to address handling and processing requirements of sensitive information.

8. Department of Forestry or its service provider shall make considerations in new or renewed contracts that address the protection of DOF or customer data on hard drives for warranty or maintenance purposes. Following are standards when maintenance or warranty is necessary:

   a. If the hard drive malfunctions and data can be removed in accordance with the requirements in this policy, the drive may be returned to the supplier for replacement under warranty or maintenance.

   b. Hard drives that are inoperable and do not allow data to be removed in accordance with the requirements in this standard, shall be physically destroyed using a method previously outlined.

Media Use (MP-7)

1. The ISO or designee:

   a. Restricts the use of non-DOF portable storage devices (such as flash drives, external storage devices) on all DOF systems.

   b. Prohibits the use of portable storage devices in DOF systems when such devices have no identifiable owner.

   c. Prohibits the use of sanitization resistant media that do not have a secure erase function/feature/tool in DOF systems.

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	6/13/2024
Director of Information Technology Name (Print)	Director of Information Technology Signature	
Amanda Davis	DocuSigned by: amanda davis C2CCAB60F85A4A6	6/13/2024
Chief of Administration Name (Print)	Chief of Administration Signature	

Version History

Version History			
Date	**Version**	**Details**	**Author/Contributors**
June 11, 2024	1	Original – CSRM template and updated with SEC530	Catherine Shefski, ISO