**Media Protection Policy Template**

# PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that “YOUR AGENCY NAME” develops, disseminates, and updates the IT Media Protection Policy. This policy and procedure establishes the minimum requirements for the IT Media Protection Policy.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.10 Media Protection Family, Controls MP-1 through MP-6, to include specific requirements for the Commonwealth of Virginia.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners) as well as all “YOUR AGENCY NAME” systems classified as sensitive.

# 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

SEC501: Information Security Standard 501

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The IT Media Protection Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the media protection requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices. This policy directs that “YOUR AGENCY NAME” meet these requirements for all sensitive IT systems.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

1. Responsible (R) – Person working on activity
2. Accountable (A) – Person with decision authority and one who delegates the work
3. Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4. 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 SEC501, MP-1 through MP-6, “YOUR AGENCY NAME” 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 “YOUR AGENCY NAME” and its customers.

1. **MEDIA PROTECTION POLICY AND PROCEDURES**
	1. The ISO or designee shall document and implement Data Storage Media protection practices. At a minimum, these practices must include the following components:
		1. Define protection of stored sensitive data as the responsibility of Data Owner.
		2. 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.
			1. The exception shall include 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; and
				5. Identification of any residual risks.
		3. 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.
		4. 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.
			1. “YOUR AGENCY NAME” employees are allowed to bring personal IT assets onto “YOUR AGENCY NAME” or business partner premises that house COV IT systems and data although personal IT assets may not be connected to the “YOUR AGENCY NAME” or business partner network.
		5. 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.
2. **MEDIA ACCESS**
	1. The ISO shall or 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).

* 1. Assessment of risk must guide the selection of media, and associated information contained on that media requiring restricted access.
	2. 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.
1. **MEDIA STORAGE**
	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:
		1. Employing cryptographic mechanisms to protect information in storage where the data is sensitive as related to confidentiality. Where encryption is not a viable option, mitigating controls and procedures must be implemented and documented;
			1. The strength of mechanisms is commensurate with the classification and sensitivity of the information.
			2. Encryption requires documented approval from the agency head.
		2. Physically controlling and securely storing digital and non-digital media within organization-defined controlled areas using organization-defined security measures; and
		3. Protecting information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
2. **MEDIA TRANSPORT**
	1. The ISO requires that:
		1. All digital and non-digital media is protected and controlled during transport outside of controlled areas using organization-defined security measures (i.e., locked container, cryptography);
			1. “YOUR AGENCY NAME” employees are responsible for safeguarding any IT assets they remove from “YOUR AGENCY NAME” 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.
		2. Accountability for information system media is maintained during transport outside of controlled areas; and
			1. “YOUR AGENCY NAME” employees must immediately report loss or theft of any IT assets assigned to them to their supervisor and to the ISO.
		3. Activities associated with transport of such media are restricted to authorized personnel.
			1. “YOUR AGENCY NAME” employees shall not remove “YOUR AGENCY NAME” 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.
		1. At a minimum, any log or tracking mechanism must include:
			1. Description of information being transported.
			2. Type of information (e.g., PII) contained on the media.
			3. Method(s) of transport.
			4. Protection measures employed.
			5. Name(s) of individual(s) transporting the information (if appropriate).
			6. Authorized recipient(s).
			7. Dates sent and received.
		2. In instances where it is necessary to remove or transport sensitive document(s) or media outside of controlled areas of “YOUR AGENCY NAME”, ISO approval must be obtained and documented.
		3. Before transporting, delivering, or mailing media containing sensitive information, individuals shall:
			1. Notify the entity authorized to receive the information.
			2. 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.
		4. Media containing sensitive information transported by a common carrier must use an acknowledgement of receipt.
		5. Personnel transporting sensitive information by car shall store the media in a locked trunk while en route.
			1. If a trunk is not available in the vehicle, the media must be hidden from sight.
			2. Personnel are prohibited from leaving media containing sensitive information in a vehicle overnight.
			3. 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.
		1. Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.
	4. Approved cryptographic mechanisms must be employed to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Note: This requirement also applies to mobile devices. Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones).

1. **MEDIA SANITIZATION**
	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.
		1. Media sanitization and disposal actions must be tracked, documented, and verified.
		2. 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).
		3. Sanitization of portable, removable storage devices must be completed prior to connecting such devices to the information system.
		4. Sanitization of portable, removable storage devices, must be considered when:
			1. Such devices are first purchased from the manufacturer or vendor prior to initial use; or
			2. When the organization loses a positive chain of custody for the device.
		5. An assessment of risk must guide the specific circumstances for employing the sanitization process.
		6. Information system media must be destroyed that cannot be sanitized.
		7. 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).
			1. Data Owners of data residing on “YOUR AGENCY NAME” 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 “YOUR AGENCY NAME” and “YOUR AGENCY NAME” 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.
				7. The effectiveness of the data removal process shall be tested by a quality assurance function independent of the organizational unit performing the data removal.
	2. One of the following three acceptable methods shall be used for the removal of data from hard drives:
		1. 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.
			1. The overwriting process including the software products and applications used for the overwriting process shall include the following steps:
			2. 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.
			3. 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.
			4. 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.
			5. 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.
			6. Sectors not overwritten shall be identified and if they cannot be removed overwriting is not acceptable and another method must be employed.
		2. 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.
			1. 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.

* + 1. 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.
			1. Hard drives shall be destroyed when they are defective or cannot be repaired or “YOUR AGENCY NAME” or Customer data cannot be removed for reuse.
			2. 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.
			3. The hard drive should then be subjected to physical force (pounding with a sledge hammer) or extreme temperatures (incineration) that will disfigure, bend, mangle or otherwise mutilate the hard drive so it cannot be reinserted into a functioning computer.
			4. 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.
	1. Electronic devices that hold user data or configurations in non-volatile memory shall have all “YOUR AGENCY NAME” 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.
	2. 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.
	3. The effectiveness of the data removal process shall be tested by a quality assurance function independent of the organizational unit performing the data removal. The quality assurance tester shall test for effective data removal for electronic media once the data has been removed or otherwise made unreadable. If more than one device has had the data removed, a sample of each device type can be tested as opposed to testing every device. The sample should include each type of electronic media (i.e., hard drives of personal computers, Personal Digital Assistants (PDAs), routers, firewalls, switches, tapes, diskettes, CDs, DVDs, worm devices, printers, and Universal Serial Bus (USB) data storage devices). The sample size for each device type should be commensurate with the sensitivity and risk of the type of data stored but must be at least 10% of the total number of devices for each type of electronic media.
		1. The testing must be documented including date, tester(s), total number of devices in the lot, number tested, method of testing and the result. Testing must be performed within 1 week of the data removal. Test methods may include physical observation if the data removal method was physical destruction or attempting to boot up and read data if the method was overwriting.
	4. “YOUR AGENCY NAME” or the “YOUR AGENCY NAME” 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.
		1. The removal of Commonwealth data must be performed and documented as required in the COV ITRM Standard ([SEC514](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/COV%20ITRSEC514-03_Data_Removal2008.pdf)).
		2. The certification form must be completed and a copy affixed to the hard drive as required in the COV ITRM Standard ([SEC514](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/COV%20ITRSEC514-03_Data_Removal2008.pdf)).
	5. Recommended software for the removal of commonwealth data from hard drives and electronic media is covered in the COV ITRM Standard ([SEC514](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/COV%20ITRSEC514-03_Data_Removal2008.pdf)).
	6. If recovery of data contained on an electronic storage media is required, “YOUR AGENCY NAME” or its service provider must provide adequate controls commensurate with the sensitivity of the data contained on the storage media as follows:
		1. 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.
		2. “YOUR AGENCY NAME” may require a non-disclosure agreement and/or confidentiality agreement in order to strictly enforce the privacy of the data.
		3. If the media must be removed from “YOUR AGENCY NAME” or Customer premises and sent offsite for recovery, “YOUR AGENCY NAME” 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.
	7. “YOUR AGENCY NAME” or its service provider shall make considerations in new or renewed contracts that address the protection of “YOUR AGENCY NAME” or Customer data on hard drives for warranty or maintenance purposes. Following are standards when maintenance or warranty is necessary:
		1. 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.
		2. 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.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” Information Security Program Policy

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO”““YOUR AGENCY NAME””)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

 [ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| Version History |
| --- |
| Version | Date | Change Summary  |
| 1 | 07/01/2014 | Supersedes “YOUR AGENCY NAME” CSRM Removal Data Hard Drives Electronic Media Policy Procedure and “YOUR AGENCY NAME” CSRM IT Asset Management Policy. |
| 2 | 11/16/2021 | Formatting changes |
|  |  |  |
|  |  |  |