1. Purpose

To establish policy for effectively handling and securing media in a manner that protects the confidentiality and integrity of data maintained on digital and non-digital media. Additionally, to establish media use restrictions and media labeling, storage, and transportation requirements to ensure the security of media outside of controlled areas. Further, to document media sanitization requirements prior to the media being disposed, reused, or released out of agency control.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments1 (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state information systems and data, whether operated or maintained by the state or on behalf of the state. For this policy, the term "agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

Media
A medium for storing data, both digital and non-digital. Digital media includes internal and external hard disk drives, flash storage drives, optical media (CDs, DVDs), and magnetic media (diskettes, magnetic tapes). Non-digital media includes paper and microfilm.

Sanitize
A process by which data is irreversibly removed from media being disposed, reused, or released out of agency control such that there is reasonable assurance the data cannot be retrieved or reconstructed. Media sanitization methods include overwriting, degaussing, and physically destruction.

---

1 State of Rhode Island Executive Branch Departments does not include the University of Rhode Island, the State colleges, the General Treasurer, the Attorney General, or the Secretary of State.
4. Procedures for Compliance

Security controls in this policy will be implemented in accordance with the security categorization of the information system. The security categorization is based on the Information Assurance Level (IAL) requirements of the information system.

Low Risk Systems (IAL1)
Information systems that only contain data that is public by law or directly available to the public via mechanisms such as the internet. In addition, desktops, laptops, and supporting systems used by agencies are Low Risk unless they store, process, transfer, or communicate private or sensitive data.

Moderate Risk Systems (IAL2)
Information systems that store, process, transfer, or communicate private or sensitive data or have a direct dependency on a Moderate system. At a minimum, any information system that stores, processes, transfers, or communicates PII or other sensitive data types is classified as a Moderate system.

4.1. [IAL1, IAL2] Media Protection Policy and Procedures (MP-1). The agency will develop, document, review, and annually update a media protection policy and procedures. Media protection policy and procedures will be disseminated to designated personnel defined in the applicable system security plan, agency information managers (AIM), technical support managers (TSM), data owners, system owners, system administrators, and any other personnel or roles the agency determines require access.

4.2. [IAL1, IAL2] Media Access (MP-2). The agency will restrict access to media containing non-public data to personnel authorized to access the data maintained on the media.

4.3. [IAL2] Media Marking (MP-3). The agency will label media containing non-public data in accordance with the type and sensitivity of the data maintained on the media, with appropriate handling instructions, distribution limitations, and any applicable security markings. Exemptions from this control must be approved in writing by the ETSS CIO.

4.4. [IAL2] Media Storage (MP-4). The agency will:
   1. Physically control and securely store media containing non-public data within controlled areas that are only accessible to individuals authorized to access the information. Digital media containing sensitive or confidential data will be encrypted using a FIPS 140-2 validated encryption module. Non-digital media containing sensitive or confidential information will be locked within a cabinet, container, safe, room, or other secured area.
   2. Protect media until it is destroyed or sanitized in accordance with ETSS policies, procedures, and standards.

4.5. [IAL2] Media Transport (MP-5). The agency will:
1. Protect and control media containing non-public data when transported outside of controlled areas. At a minimum, media containing sensitive or confidential data will be:

   a. Encrypted using a FIPS 140-2 validated encryption module.
   b. Transported using tamper-proof packaging (e.g. locked container, sealed envelope).
   c. If hand-carried, secured within a secure container (e.g. locked briefcase) by authorized personnel.
   d. If shipped, provided a trackable receipt from a commercial carrier.
   e. Secured within secure containers at all times during transport.

2. Maintain accountability of media containing non-public data when transported outside of controlled areas.

3. Document activities associated with the transport of media.

4. Restrict the transport of media to authorized personnel.

4.5.1. [IAL2] Cryptographic Protection (MP-5.4). The information system will implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media, including mobiles devices with storage capability, during transport outside of controlled areas.

4.6. [IAL1, IAL2] Media Sanitization (MP-6). The agency will:

   1. Sanitize media containing non-public data prior to disposal, reuse, or release out of agency control, including:
      a. Media that, at any point during its lifecycle, contained non-public data and there is no certification that the non-public data was previously sanitized.
      b. Media requested as part of an investigation, litigation, audit, or other similar type of action to reflect the requirements of the request.
      c. Media that is under vendor warranty prior to exchanging the media with the vendor.
General Media Sanitization Process

2. Employ an ETSS approved sanitization method (i.e. overwrite, degauss, physically destroy) that is appropriate for and commensurate with the security requirements, media operability, and sensitivity of the data. In general:
   a. Media that is in operable condition and intended to be reused, either by the agency or another state agency, will be overwritten prior to being recommissioned and placed back into use.
   b. Media that is not operable, has reached the end of its useful life, is intended to be completely removed from service, or cannot be properly sanitized by overwriting will be degaussed or physically destroyed, as appropriate.
   c. Dispose of the electronic equipment in accordance with DCAMM surplus policies and standards.

---

**ETSS Approved Sanitization Methods**

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overwrite</td>
<td>Replacing existing data on digital media with other data (such as all “0” or “1” everywhere on the media) to essentially &quot;erase&quot; the existing data. Multiple passes and specific overwriting patterns are used to prevent advanced data recovery techniques from taking advantage of data remanence (the residual representation of digital data even after attempts to erase the data).</td>
<td>Sanitize the entire disk drive (independent of the BIOS, operating system, or any firmware capacity limitation) to make it impossible to recover any meaningful data. Perform a minimum of three (3) overwrite passes of all sectors, blocks, tracks, or unused disk space.</td>
</tr>
<tr>
<td>Degauss/Overwrite/Physically Destroy</td>
<td>Degauss/Overwrite, as appropriate. If physically destroying, degauss/overwrite first.</td>
<td></td>
</tr>
<tr>
<td>Non-rotating disk storage media?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Magnetic media?</td>
<td>Rotating disk storage media?</td>
<td>No</td>
</tr>
<tr>
<td>Optical media?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Paper/Microform media?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Does media contain confidential, sensitive, or private data? Must confidentiality be maintained?</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

---

**Start**

**End**

Document Log sanitized media (see "Media Sanitization Log").

Physically Destroy

Cross-cut shred to 1mm x 5mm.

Physically Destroy

Shred, pulverize, or incinerate. Remove or grind off information-containing layer first.

Degauss/Overwrite/Physically Destroy

Degauss/Overwrite, as appropriate. If physically destroying, degauss/overwrite first.

Overwrite/Physically Destroy

Overwrite, as appropriate. If physically destroying, overwrite first.

Observe degaussing machine

Ensure media is sanitized.

Validate

Ensure media is sanitized.

Start

Does media contain confidential, sensitive, or private data? Must confidentiality be maintained?

Paper/Microform media?

Yes

No

Optical media?

Yes

No

Magnetic media? Rotating disk storage media?

Yes

No

Non-rotating disk storage media?

Yes

No

Identify the final disposition of media (surplus, trash, reusing, transferring to another agency) to determine the most appropriate sanitization method.

Sanitize the entire disk drive (independent of the BIOS, operating system, or any firmware capacity limitation) to make it impossible to recover any meaningful data.

Perform a minimum of three (3) overwrite passes of all sectors, blocks, tracks, or unused disk space.

Use of a strong magnet to demagnetize

Observe degaussing machine
magnetic media and realign the magnetic field, essentially erasing the data. Most magnetic media is rendered useless following the degaussing process. Use degaussing machine at full magnetic strength. Remove shielding materials (cabinets, mounting brackets) and hard disk platters with a high coercivity (a measure of magnetic medias resistance to becoming demagnetized) prior to degaussing.

<table>
<thead>
<tr>
<th>Physical Destruction</th>
<th>Example</th>
<th>Sanitization Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any method that physically destroys digital/non-digital media to render data unrecoverable, such as shredding (cut/break media into very small pieces), pulverizing (grind media into a powdery consistency), or incinerating (burn media at high temperatures into an ash-like consistency)</td>
<td>Physically destroy digital media that is defective or that cannot be properly overwritten or repaired.</td>
<td>Shred non-digital media containing confidential, sensitive, or private data to a maximum particle size of 1mm x 5mm using a cross-cut shredder prior to being disposed.</td>
</tr>
</tbody>
</table>

### ETSS Recommended Sanitization Methods for Media

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Example</th>
<th>Sanitization Method</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rotating Disk Storage</strong></td>
<td>ATA, SATA, SCSI, and other rotating hard disk storage media found in computers, servers, SANs, printers, copiers, external/portal drives, etc.</td>
<td>Overwrite, Degauss, Physically Destroy</td>
</tr>
<tr>
<td><strong>Non-Rotating Storage</strong></td>
<td>SDD, flash, and other non-rotating non-magnetic storage media found in flash drives, memory cards, SD cards, PDA, smartphones, digital cameras/recorders, etc.</td>
<td>Overwrite, Physically Destroy</td>
</tr>
<tr>
<td><strong>Magnetic</strong></td>
<td>Soft disk and tape storage media such as floppy/ZIP disks, LTO/DLT tapes, audio/video tapes/cassettes, etc.</td>
<td>Overwrite, Degauss, Physically Destroy</td>
</tr>
<tr>
<td><strong>Optical</strong></td>
<td>Storage media read by laser such as optical disks, CDs, DVDs, Blu-rays, etc.</td>
<td>Physically Destroy</td>
</tr>
<tr>
<td><strong>Paper</strong></td>
<td>Any paper document with non-public data.</td>
<td>Physically Destroy</td>
</tr>
<tr>
<td><strong>Microform</strong></td>
<td>Micro-reproductions of images or documents such as microfilm, microfiche, etc.</td>
<td>Physically Destroy</td>
</tr>
</tbody>
</table>

3. Validate media prior to final disposition to ensure data has been erased and no meaningful data is recoverable.

4. Maintain a media sanitization log regarding final disposition of media. Media sanitization records will include (regardless if media is sanitized in-house or by a third party) the following:
   a. Name, agency, and signature of individual authorizing sanitization.
b. Name, agency, and signature of individual receiving media and accountable for sanitization of the media (provide info for external party if an external party is performing sanitization).

c. Date media received.

d. Media description (ex. make/model, hard drive, SATA drive, CD).

e. Media control number, if available (ex. serial number, state asset tag ID).

f. Description of media contents.

g. Sanitization method used (ex. overwrite, degauss, physically destroy).

h. Disposition of media following sanitization (ex. surplus, trash, re-using, transfer to another agency).

i. Date of disposition.

5. Third party providers contracted to sanitize media and other similar information destruction services must adhere to the requirements of this control and be certified by the National Association for Information Destruction (NAID).

4.7. [	ext{IAL1}, \text{IAL2}] Media Use (MP-7). The agency will:

1. Establish media use restrictions for accessing and connecting media to information systems and system components. Non-state-owned media and storage devices are prohibited from connecting to the network or information system without prior formal written authorization from the system owner and ETSS CISO.

2. Prohibit the use of portable storage devices within agency information systems when the device does not have an identifiable owner (e.g. authorized individual, agency).

4.7.1. [	ext{IAL2}] Prohibit Use Without Owner (MP-7.1). The agency will prohibit the use of portable storage devices within agency information systems when such devices have no identifiable owner.

5. Approval / Review Signature:

```
Digitally signed by Brian Tardiff
Date: 2021.10.25 12:27:08 -04'00'
```

Chief Information Security Officer