|  |  |
| --- | --- |
| **Data Sanitization Policy** | **No. [Organization Name] IS-8** |
|  | **Effective Date:** March 30, 2023 |

1. **Overview**

When files are improperly or inadequately purged from storage media, it is often still possible to reconstruct or retrieve data. To mitigate the potentially significant risk of unauthorized disclosure of [Organization Name] data, storage media must be appropriately sanitized to prevent unauthorized access to or disclosure of sensitive institutional data.

In addition to being a widely accepted security and privacy practice, effective media sanitization is required by federal and state regulations following the NIST and NSA standards. Data must be permanently erased or purged from endpoint devices such as computers, laptops, printers, cell phones, and digital communications equipment) or centralized storage media such as servers and arrays containing server hard drives, data tapes and solid state drives. The third category of data storage is USB, optical drives, and externals drives. Effective media sanitization requires the application of certified techniques to prevent recovery or reconstruction of residual stored data on the media. Any data sanitization is only valid with verification by a second qualified person who can sign a Certificate of Destruction per the NIST guidelines.

1. **Purpose**

Adopted by both federal and state regulations, the Media Protection (MP) section of the NIST standard focuses on the organization to review, approve, track, document, and verify media sanitization and disposal action as well as specific data destruction techniques. That means that when a failed or decommissioned data bearing device is placed out of action, the organization needs a system that is compliant to prove that when the physical device is now sanitized of all [Organization Name] data, that there is no chance that the sensitive data or means to connect to the [Organization Name] network to gain data is possible.

Multiple studies have found that the use of using free ware or not following strict protocols that remarketed endpoint devices, servers and firewalls still contain enterprise data.

1. **Scope**

This Data Sanitization Policy applies to the [Organization Name]. It further applies to:

* 1. Personal owned devices that have stored [Organization Name] data.
  2. Employees that changes positions from one Zone to another or leaves the [Organization Name]
  3. Any storage media that has been used to store [Organization Name] digital or electronic information or data even temporarily
  4. Storage media that maintain data exclusively classified as Low Risk can utilize the least rigorous technique of sanitization prior to transfer or disposal
  5. Storage media being transferred within the [Organization Name], returned, or disposed of at the conclusion of a lease, or disposed of at the end of its useful life. Lease agreements should state that although the device is to be returned, no internal data bearing device can leave the control of the [Organization Name]
  6. Any third-party provider with a contractual relationship with the [Organization Name] that maintains the same data types.

1. **Policy**

Sanitization is defined as the erasure, overwriting, or physical destruction of storage media to the extent that data cannot be recovered using normal system functions or software data recovery utilities. Unless otherwise proven, it is assumed that all [Organization Name] owned devices have stored at a minimum data classified as **Restricted**. Consequently, all [Organization Name] owned devices must be sanitized according to this policy at their end-of-life or prior to disposal or recycling. Specifically, no device or storage media containing Personally Identifiable Information (PII), or any data classified as **Restricted** can be transferred or disposed of without following physical destruction of the internal data bearing device.

[Organization Name] Property Disposition has sole responsibility for the disposition of [Organization Name]-owned property. Individuals with [Organization Name] owned devices must either

a) Sanitize and verify the devices using the procedure and method described below, or

b) Have [Organization Name] IT department do the sanitizing and verifying

Contractual agreements cannot negate the responsibility to individuals to allow [Organization Name] data to leave the control of the [Organization Name].

The primary responsibility for sanitizing computer systems, electronic devices, and media rests with the [Organization Name] CISO.

* 1. **Moving a Data Bearing Device Out of Service**

Individuals must request through the [Organization Name] manager to remove an endpoint device out of service. In the request, the attributes to be captured for the device will meet the NIST SP 800-88 standard.

1. [Organization Name] Asset Tag Number
2. Serial number of data bearing device
3. Description of the device (Tablet, hard drive, solid state drive, etc)
4. Manufacturer
5. Model
6. Hostname for data bearing devices
7. Date of leaving service

If the device does not have an [Organization Name] Asset Tag number, it will be assigned one with the request. The [Organization Name] CISO office will determine if data on the device needs to be migrated to another [Organization Name] storage device prior to data destruction.

* 1. **Containing the Data Bearing Device**

The [Organization Name] data bearing device will be logged into and contained in a locked safe until data destruction is scheduled. The [Organization Name] data bearing device is to be maintained until permission is given for data sanitization.

Hardware tracking of [Organization Name] IT equipment includes the inventory of data bearing devices in containment.

* 1. **Data Sanitization of the Data Bearing Device**

End of Life data sanitization should follow the NSA physical standard for data destruction and the NIST standard for documentation.

Physical destruction of [Organization Name] data bearing devices onsite in the [Organization Name] control as follows:

**Magnetic Hard Drive** Degauss the data bearing device with an NSA certified degausser for 5000oe. Deform the hard drive platters

**Magnetic Data Tape** Degauss the data bearing device with an NSA certified degausser for 5000oe. Shred the data tape to destroy the data tape physically

**Solid State Media** Shred the solid-state components to 2 mm particle size using an NSA certified 2 mm shredder

* + 1. **Overwrite**

Overwriting the solid-state data bearing devices can be conducted only if the [Organization Name] data bearing device never contained **Restricted** data.

Overwriting solid state devices need to use software that is approved by the [Organization Name] CISO office. A copy of the third-party verification of the overwrite software is required to be on file in the [Organization Name] CISO office.

Note: Overwrite software is designed and tested for certain devices and are typically not universal, so only trained and certified media sanitization specialist with certification on file in the [Organization Name] CISO office are permitted to sanitize or verify [Organization Name] data bearing devices.

* 1. **Verification of the Data Sanitization**

100% verification of the data sanitization process is required. It can be accomplished as follows:

1. Visual verification of the physical destruction by a second team member
2. Testing of the data bearing device to try to recover data
   1. **Data Sanitization Report**

Data sanitization reports are as follows:

1. Certificate of Destruction per the NIST SP 800-88 standard are typically electronic since hundreds of data bearing devices can be processed at a time. The Certificate of Destruction will have the following attributes:
2. Manufacturer
3. Model
4. Serial Number
5. [Organization Name] Asset Tag Number
6. Media Type (i.e., magnetic, flash memory, hybrid, etc.)
7. Media Source (i.e., user or computer the media came from)
8. Pre-Sanitization Data Classification Categorization
9. Sanitization Description (Clear, Purge, Destroy)
10. Method Used (degauss, overwrite, block erase, crypto erase, etc.)
11. Tool Used (including version)
12. Verification Method (i.e., full, quick sampling, etc.)
13. Post-Sanitization Destination
14. Name of Sanitizer
15. Title of Sanitizer
16. Signature of Sanitizer
17. Name of Verifier
18. Title of Verifier
19. Signature of Verifier
20. Date and Time of Data Sanitization
21. Certificate of Recycling from a R2, e-steward or ISO 14001 recycler

* 1. **Data Sanitization Training**

Like procedures for software updates, data sanitization is often done partially because it is a task that requires 100% accuracy. Data sanitization training should include the following:

1. Overwriting module
2. Encryption – erase module
3. Degauss module
4. Solid state shredding module
5. Verification module
6. E-waste safety module
   1. **Data Sanitization Management Review**

The [Organization Name] CISO office is required to issue a balance report that accounts for all [Organization Name] data bearing devices annually.

Loss of control of data bearing devices is considered a data breach and should be handled using the [Organization Name] Incident Management and Response Policy.

# **Policy Compliance**

* 1. **Compliance Measurement**

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

# **Exceptions**

Any exception to the policy must be approved by the Infosec team in advance.

# **Non-Compliance**

An end user found to have violated this policy may be subject to disciplinary action, up to and including termination of appointment to the [Organization Name].

# **Related Standards, Policies and Processes**

United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53r5 Security and Privacy Controls for Federal Information Systems and Organizations, April 2013

* MA-02 (d) Controlled Maintenance
* MA-03 (3)(b) Maintenance Tools
* MA-05 (1)(a)(2),(1)(b) Media Transport
* MP-04 (b) Media Storage
* MP-06 Media Sanitization
* MP-7 (2) Media Use
* MP-8 (4) Media Downgrading
* SC-4 (2) Information in Shared Resources

United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-88r1 Guidelines for Media Sanitization, December 2014

Federal Information Processing Standards Publication (FIPS) 140-2: Security Requirements for Cryptographic Modules

[Organization Name] Incident Management and Response Policy

# **Definitions and Terms**

None

# **Revision History**

|  |  |  |
| --- | --- | --- |
| Date of Change | Responsible | Summary of Change |
| March 30, 2023 | [Organization Name] | Created initial draft |
|  |  |  |