|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **Sanitization and Secure Disposal** | **Updated:** 10/29/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

Information systems capture, process, and store information using a wide variety of media, including paper. This information is not only located on the intended storage media but also on devices used to create, process, or transmit this information. These media may require special disposition in order to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

According to the Information Security Policy, information must be managed from creation to secure disposal. Users and custodians must understand the sensitivity of information and the requirements for media sanitization and disposal. All workforce members, including property management and custodial staff, should be informed of these processes to ensure accountability. Confidential materials must be destroyed only by authorized personnel using approved methods. Service providers may be used for destruction, provided they maintain security until completion and comply with this standard. Maintenance and contractual agreements must adequately protect the confidentiality of information based on classification standards.

* 1. Methods of Media Sanitization

The following table depicts the three types of sanitization methods and the impact of each method.

| **Sanitization Method** | **Appropriate Use** | **Description** |
| --- | --- | --- |
| Clear | If the media will be reused and will not be leaving the entity’s control. | Protects confidentiality of information against an attack by replacing written data with random data. Clearing must not allow information to be retrieved by data, disk or file recovery utilities. |
| Purge | If the media will be reused and leaving the entity’s control. | Protects confidentiality of information against an attack through either degaussing or Secure Erase. |
| Physical Destruction | If the media will not be reused at all. | Intent is to completely destroy the media. |

* 1. Sanitization Decision Process

1. The decision process is based on the confidentiality of the information, not the type of media. The entities choose the type of sanitization to be used, and the type of sanitization is approved by the Information Owner. The technique used may vary by media type and by the technology available to the custodian, so long as the requirements of the sanitization type are met. Recommended Sanitization techniques for specific types of media are outlined in Appendix A of NIST 800-88, Rev. 1, Guidelines for Media Sanitization, Minimum Sanitization Recommendations.
2. Disposal without sanitization should be considered only if information disclosure would have no impact on organizational mission, would not result in damage to organizational assets, and would not result in financial loss or harm to any individuals.
3. The security categorization of the information, along with internal environmental factors, should drive the decisions on how to deal with the media. The key is to first think in terms of information confidentiality, then apply considerations based on media type.



1. Figure 4.1- Sanitization and Disposition Decision Flow
2. (*from NIST 800-88, Rev. 1, Guidelines for Media Sanitization*)
3. The cost versus benefit of a sanitization process should be understood prior to a final decision. Entities can always increase the level of sanitization applied if that is reasonable and indicated by an assessment of the existing risk. For example, even though Clear or Purge may be the recommended solution, it may be more cost-effective (considering training, tracking, and validation, etc.) to destroy media rather than use one of the other options. Entities may not decrease the level of sanitization required.
   1. Control of Media

A factor influencing a sanitization decision is who has control and access to the media. This aspect must be considered when media leaves organizational control. Media control may be transferred when media are returned from a leasing agreement or are being donated or resold to be reused outside the organization. The following are examples of media control:

1. Under SE Control:
   1. Media being turned over for maintenance are still considered under the entity’s control if contractual agreements are in place and the maintenance provider specifically provides for the confidentiality of the information.
   2. Maintenance being performed on an entity’s site, under the entity’s supervision, by a maintenance provider is also considered under the control of the entity.
2. Not Under Entity Control:
   1. Media that are being exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to the entity are considered to be out of the entity’s control.
   2. Media Sanitization Reuse of Media

Entities should consider the cost versus benefit of reuse. It may be more cost-effective (considering training, tracking, and validation, etc.) to destroy media rather than use one of the other options.

* 1. Clear / Purge / Destroy

Prohibit the use of [entity defined types of information system media] on entity owned equipment using unapproved security safeguards. Adhere to the following descriptions of the clearing, purging, and destruction of media:

|  |  |
| --- | --- |
| **Method** | **Description** |
| Clear | One method to sanitize media is to use software or hardware products to overwrite user- addressable storage space on the media with non-sensitive data, using the standard read and write commands for the device. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also should include all user- addressable locations. The security goal of the overwriting process is to replace Target Data with non-sensitive data. Overwriting cannot be used for media that are damaged or not rewriteable and may not address all areas of the device where sensitive data may be retained. The media type and size may also influence whether overwriting is a suitable sanitization method. For example, flash memory-based storage devices may contain spare cells and perform wear levelling, making it infeasible for a user to sanitize all previous data using this approach because the device may not support directly addressing all areas where sensitive data has been stored using the native read and write interface.  The Clear operation may vary contextually for media other than dedicated storage devices, where the device (such as a basic cell phone or a piece of office equipment) only provides the ability to return the device to factory state (typically by simply deleting the file pointers) and does not directly support the ability to rewrite or apply media-specific techniques to the non-volatile storage contents. Where rewriting is not supported, manufacturer resets and procedures that do not include rewriting might be the only option to Clear the device and associated media. These still meet the definition for Clear as long as the device interface available to the user does not facilitate retrieval of the Cleared data. |
| Purge | Some methods of purging (which vary by media and must be applied with considerations described further throughout this document) include overwrite, block erase, and Cryptographic Erase, through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands.  Destructive techniques also render the device Purged when effectively applied to the appropriate media type, including incineration, shredding, disintegrating, degaussing, and pulverizing. The common benefit across all these approaches is assurance that the data is infeasible to recover using state of the art laboratory techniques. However, Bending, Cutting, and the use of some emergency procedures (such as using a firearm to shoot a hole through a storage device) may only damage the media as portions of the media may remain undamaged and therefore accessible using advanced laboratory techniques.  Degaussing renders a Legacy Magnetic Device Purged when the strength of the degausser is carefully matched to the media coercivity. Coercivity may be difficult to determine based only on information provided on the label. Therefore, refer to the device manufacturer for coercivity details. Degaussing should never be solely relied upon for flash memory-based storage devices or for magnetic storage devices that also contain non-volatile non-magnetic storage. Degaussing renders many types of devices unusable (and in those cases, Degaussing is also a Destruction technique). |
| Destroy | There are many different types, techniques, and procedures for media Destruction. While some techniques may render the Target Data infeasible to retrieve through the device interface and unable to be used for subsequent storage of data, the device is not considered Destroyed unless Target Data retrieval is infeasible using state of the art laboratory techniques.   * *Disintegrate, Pulverize, Melt, and Incinerate*. These sanitization methods are designed to completely Destroy the media. They are typically carried out at an outsourced metal Destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. * *Shred*. Paper shredders can be used to Destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. To make reconstructing the data even more difficult, the shredded material can be mixed with non-sensitive material of the same type (e.g., shredded paper or shredded flexible media).   The application of Destructive techniques may be the only option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media, or when the verification of Clear or Purge methods fails (for known or unknown reasons). |

* 1. Validation

Entities must test a representative sampling of media for proper sanitization to assure that proper protection is maintained.

* 1. Verification of Equipment

If the entity is using sanitization tools (e.g., a degausser), the entity must have procedures to ensure that the tools are operating effectively.

* 1. Verification of Personnel Competencies

Entities must ensure that equipment operators are properly trained and competent to perform sanitization functions.

* 1. Document

Entities must maintain a record of their sanitization to document what media were sanitized, when, how they were sanitized, and the final disposition of the media.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-88 - Guidelines for Media Sanitization](https://csrc.nist.gov/pubs/sp/800/88/r1/final)