



Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	No: NYS-S13-003
IT Standard: Sanitization/Secure Disposal	Updated: 02/07/2020
	Issued By: NYS Office of Information Technology Services Owner: Chief Information Security Office

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

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117* provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, [NYS-P08-002 Authority to Establish State Enterprise Information Technology \(IT\) Policy, Standards and Guidelines](#).

3.0 Scope

This standard applies to all “State Government” entities as defined in Executive Order 117 or “State Agencies” as defined in Section 101 of the State Technology Law (“State Entities”), their employees, and all others, including third parties (such as local governments, consultants, vendors, and contractors), that use or access any ITS Information Technology Resource for which ITS has administrative responsibility,

including systems managed or hosted by third parties on behalf of the ITS. Where a conflict exists between this standard and a State Entity's standard, the more restrictive provision within the applicable standard will take precedence.

This standard covers all media containing State Entity (SE) information regardless of format or location, including that which is held by third parties on behalf of the SE. Electronic media may be contained in or be a part of personal or laptop computers, printers, scanners, fax machines, mobile devices, copiers, or other devices which may allow temporary or permanent storage of information.

This standard applies to all forms of media based on the classification of the data's confidentiality according to the [NYS-S14-002 Information Classification Standard](#), whether the data is encrypted or not. Information classification is outside the scope of this document, but without classification, the risk of an SE losing control of media containing sensitive information is greatly increased. If the SE has not identified the classification of information on media, the disposition should follow the sanitization method for confidential information.

4.0 Information Statement

As per the [NYS-P03-002 Information Security Policy](#), information must be properly managed from its creation, through authorized use, to proper disposal.

The SE must ensure that users and custodians of information are aware of its sensitivity and the basic requirements for media sanitization and secure disposal.

The SE must ensure that all workforce members, including property management and custodial staff, are made aware of the media sanitization and secure disposal process in order to establish proper accountability for all data.

The SE must ensure that confidential material is destroyed only by authorized and trained personnel, whether in-house or contracted, using methods outlined in this standard.

The SE may use service providers for destruction purposes provided that the information remains secure until the destruction is completed. The service providers must follow this standard. The SE must ensure that maintenance or contractual agreements are in place and are sufficient in protecting the confidentiality of the system media and information commensurate with the information classification standards.

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 SE'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 SE'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.

Sanitization Decision Process

The decision process is based on the confidentiality of the information, not the type of media. The SEs 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 [NIST 800-88, Rev. 1, Guidelines for Media Sanitization, Appendix A - Minimum Sanitization Recommendations](#).

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.

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.

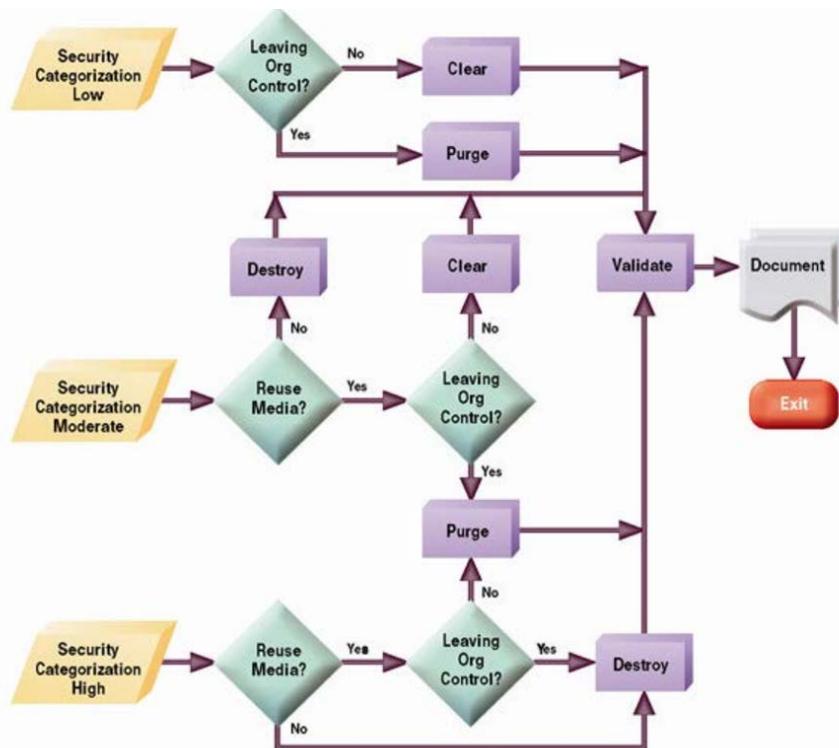


Figure 4.1- Sanitization and Disposition Decision Flow
 (from NIST 800-88, Rev. 1, Guidelines for Media Sanitization)

The cost versus benefit of a sanitization process should be understood prior to a final decision. SEs 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 verification, etc.) to destroy media rather than use one of the other options. SEs may not decrease the level of sanitization required.

Control of Media

A factor influencing an SE 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:

Under SE Control:

- Media being turned over for maintenance are still considered under SE control if contractual agreements are in place with the SE and the maintenance provider specifically provides for the confidentiality of the information.
- Maintenance being performed on an SE's site, under the SE's supervision, by a maintenance provider is also considered under the control of the SE.

Not Under SE Control:

- Media that are being exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to the SE are considered to be out of SE control.

Reuse of Media

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

Clear / Purge / Destroy

Method	Description
Clear	<p>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.</p> <p>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.</p>
Purge	<p>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.</p> <p>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.</p> <p>Degaussing renders a Legacy Magnetic Device Purged when the strength of the</p>

	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	<p>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.</p> <ul style="list-style-type: none"> • <i>Disintegrate, Pulverize, Melt, and Incinerate.</i> 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. • <i>Shred.</i> 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). <p>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).</p>

Table 5-1 – Sanitization Methods
(from NIST 800-88, Rev. 1, Guidelines for Media Sanitization)

Validation

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

Verification of Equipment

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

Verification of Personnel Competencies

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

Document

SEs 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 standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. ITS may amend its policies and standards 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, State Entities shall request an exception through the Chief Information Security Office [exception process](#).

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in <http://www.its.ny.gov/glossary>.

7.0 Contact Information

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

Chief Information Security Office
Reference: NYS-S13-003
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: <http://www.its.ny.gov/tables/technologypolicyindex>

8.0 Revision History

This standard shall be reviewed at least once every year to ensure relevancy.

Date	Description of Change	Reviewer
10/18/2013	Original Standard Release; replaces ITS S06-006 Media Disposal and Sanitization	Thomas Smith, Chief Information Security Officer
10/17/2014	Added reference to NYS-P03-002 Information Security Policy	Deborah A. Snyder, Chief Information Security Officer
06/26/2017	Updated to reference most recent version of the NIST guidelines, contact information and rebranded.	Deborah A. Snyder, Chief Information Security Officer
02/07/2020	Update to Authority, Scope and Contact Information	Karen Sorady, Acting Chief Information Security Officer

9.0 Related Documents

[NIST 800-88, Rev. 1, Guidelines for Media Sanitization](#)

[NYS-S14-002 Information Classification Standard](#)

[NYS-P03-002 Information Security Policy](#)