



ANDREW M. CUOMO
Governor

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

BRIAN DIGMAN
NYS Chief Information Officer
Director, Office of IT Services

| | |
|--|---|
| <p>New York State Information Technology Standard</p> | <p>No: NYS-S13-003</p> |
| <p>IT Standard: Sanitization/Secure Disposal</p> | <p>Updated: 10/17/2014</p> <p>Issued By: NYS ITS</p> <p>Standard Owner: Enterprise Information Security Office</p> |

1.0 Purpose and Benefits of the Standard

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 Enterprise IT Policy/Standard Statement

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the Office of Information Technology Services (ITS), 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.

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

3.0 Scope

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 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 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 four types of sanitization methods and the impact of each method.

| Sanitization Method | Appropriate Use | Description |
|---------------------|--|---|
| Dispose | If the loss of the information will have no impact on the SE (i.e. non-confidential data). | Discard media without sanitizing. |
| 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. |

| Sanitization Method | Appropriate Use | Description |
|----------------------|---|--|
| 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. Once SEs decide what type of sanitization is best, the media type will influence the technique used to achieve sanitization. Sanitization techniques are outlined in Appendix A of NIST 800-88, Guidelines for Media Sanitization.

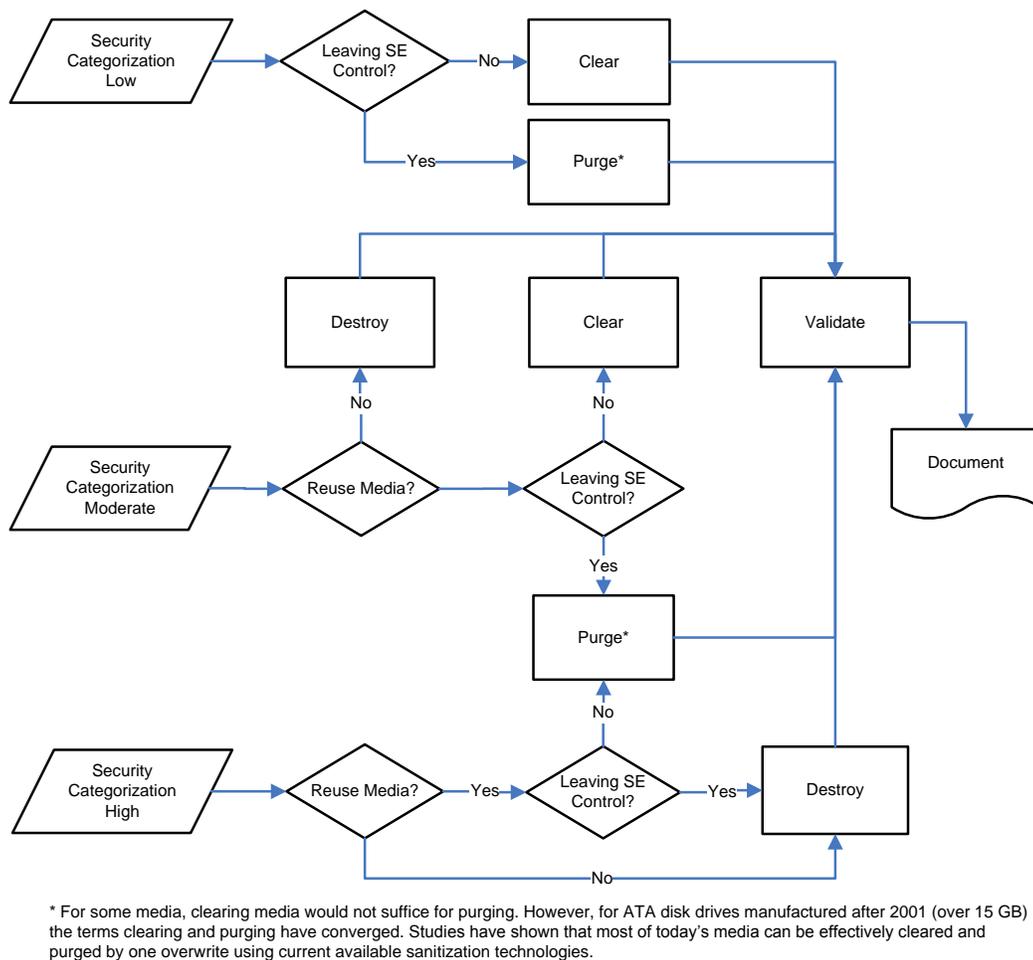


Figure 4.1- Sanitization and Disposition Decision Flow
(from NIST 800-88, Guidelines for Media Sanitization)

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 validation, 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 validation, etc.) to destroy media rather than use one of the other options.

Clear / Purge / Destroy

| Method | Description |
|---------|---|
| Clear | One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method. |
| Purge | Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. |
| Destroy | There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack. <ul style="list-style-type: none">• <i>Disintegration, Pulverization, Melting, and Incineration.</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>Shredding.</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. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be |

| | |
|--|---|
| | reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm ²). |
|--|---|

Figure 4.2 – Sanitization Methods
 (from NIST 800-88, 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. The Policy Unit shall review the standard at least once every year to ensure relevancy. The Office may also assess agency compliance with this standard. To accomplish this assessment, ITS may issue, from time to time, requests for information to covered agencies, which will be used to develop any reporting requirements as may be requested by the NYS Chief Information Officer, the Executive Chamber or Legislative entities.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, SEs shall request an exception through the Enterprise Information Security Office exception process.

6.0 Definitions of Key Terms

Not applicable

7.0 ITS Contact Information

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

Standard Owner
Attention: Enterprise Information Security Office
New York State Office of Information Technology Services
1220 Washington Avenue – Bldg. 7A, 4th Floor
Albany, NY 12242
Telephone: (518) 242-5200
Facsimile: (518) 322-4976

Questions may also be directed to your ITS Customer Relations Manager at:

Customer.Relations@its.ny.gov

The State of New York Enterprise IT Policies may be found at the following website:

<http://www.its.ny.gov/tables/technologypolicyindex.htm>

8.0 Review Schedule and Revision History

| Date | Description of Change | Reviewer |
|-------------|--|--|
| 10/18/2013 | Original Standard Release; <i>replaces ITS S06-006 Media Disposal and Sanitization</i> | 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 |
| 10/17/2015 | Scheduled Standard Review | |

9.0 Related Documents

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