Disposal of Media Storage Device Procedure

1. Purpose

   This procedure identifies the steps used for disposing of media storage devices. It meets the requirements for the State Enterprise Information Security Policy.
   It is a requirement to protect IT assets by 1) destruction of the IT device or 2) complete removal of all electronic data from the media storage devices.

2. Policy
   Disposal of Media Storage Device Procedure applies to the following controls found within the Information Security Policy.
   a. Information Security Policy
      - Protect
        - 2.9.3.4
        - 2.13
        - 2.18.3

   b. Information Security Policy – Appendix A
      - Media Protection (MP)
        - MP-4 – Media Storage
        - MP-6 – Media Sanitization

3. Recommended Best-Practices to be Adopted as Standard Configuration

Media Storage Device is defined by any device that stores and records data. Examples may include; internal and external hard-drives in workstations, servers, printers, copiers, portable storage devices (USBs), laptops, tablets, CD's, DVD's, audio recorders, memory, etc.

All media storage devices must be sanitized prior to disposal. If sanitization cannot be completed, the media storage must be reset to factory state or destroyed. Media storage on leased equipment may be destroyed before equipment is returned.

Agency IT personnel should use a sanitation program that complies with NIST requirements and will effectively sanitize the media storage device. Employed sanitation mechanisms (strength and integrity) must meet the classification and sensitivity of the information.

Destruction process:

1. In the event a disk cannot be properly wiped because it is failing or not compatible with our wiping process, it is sent to Ewaste.
2. The Ewaste partner destroys all disks with their disk shredder.
3. All destruction must be completed on site.

Solid state drives must be sanitized using an authenticated tool. The wiping will be validated and tape will be placed over the drive to identify that the device has been wiped.

If a device cannot be sanitized, the system will be destroyed.

Documentation
Agency directors are responsible for maintaining documentation on all electronic data storage devices (e.g., PCs, laptops, servers, portable devices) that have been either destroyed or sanitized. These records must be retained by the agency for six years. The disposal records shall contain the following information:

1. Employee name performing cleaning
2. Date of cleaning
3. Device Type
4. Device(s) identification (vendor serial number or Dell service tag number)

5. Method of Sanitization
6. Destination of device
7. Disposing Agency

Summary of Sanitization Methods

Table 5-1: Sanitization Methods

Method	Description
Clear	One method to sanitize media is to use software or hardware products to overwrite useraddressable 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 useraddressable 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).
Method	**Description**
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).

Sanitization and Disposition Decision Flow

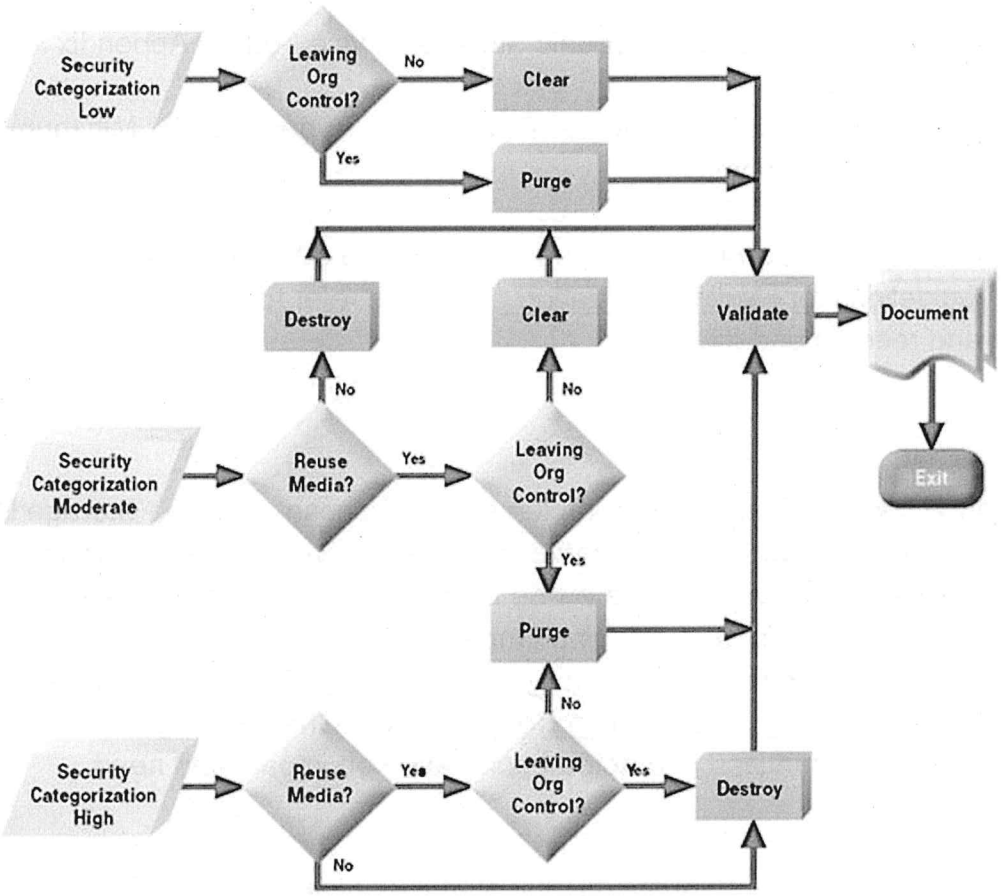

Figure 4-1: Sanitization and Disposition Decision Flow

Minimum Sanitization Recommendations

See Disposal of Computer or Electronic Storage Device Form – Appendix A

See Disposal of Media Storage Device Procedure – Appendix B for Minimum Sanitization Recommendations.

Recommendations are from NIST Special Publication 800-88 Revision 1 (December 2014) - Guidelines for Media Sanitization. **Please refer to NIST for most current version and recommendations.

4. Compliance

Compliance shall be evidenced by implementing Disposal of Media Storage Device as described above. Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this Disposal of Media Storage Device procedure are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

Definitions:
Terms and definitions are identified in the National Institute of Standards and Technology (NIST) Glossary of Key Information Security Terms and Guidelines for Media Sanitization.

References:
NIST Special Publication 800-88 Revision 1 (December 2014) - Guidelines for Media Sanitization

Appendix A

MT-ISAC Best Practice

Disposal of Computer or Electronic Storage Device Form

Disposal Information

Individual responsible for cleaning: Click here to enter name	Date: Click here to enter a date.
Device Type: Choose an item.	Asset Number(s):
Method of Sanitization or Destruction: Choose an item.	
Destination of device: Choose an item.	If selected Other please explain: Click here
Sanitized by (type name):	
Disposing Agency:	
Comments: Click here	

Appendix B

Minimum Sanitization Recommendations

Recommendations are from NIST Special Publication 800-88 Revision 1 (December 2014) - Guidelines for Media Sanitization. **Please refer to NIST for most current version and recommendations.

Table A-1: Hard Copy Storage Sanitization

Hard Copy Storage	
Paper and microforms	
Clear:	N/A, see Destroy.
Purge:	N/A, see Destroy
Destroy:	Destroy paper using cross cut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller), or pulverize/disintegrate paper materials using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen. Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning.
Notes:	When material is burned, residue must be reduced to white ash.

Table A-2: Networking Device Sanitization

Networking Devices	
Routers and Switches (home, home office, enterprise)	
Clear:	Perform a full manufacturer's reset to reset the router or switch back to its factory default settings.
Purge:	See Destroy. Most routers and switches only offer capabilities to Clear (and not Purge) the data contents. A router or switch may offer Purge capabilities, but these capabilities are specific to the hardware and firmware of the device and should be applied with caution. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.

Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	For both Clear and (if applicable) Purge, refer to the manufacturer for additional information on the proper Sanitization procedure. Network Devices may contain removable storage. The removable media must be removed and sanitized using media-specific techniques.

Table A-3: Mobile Device Sanitization

Mobile Devices **(If a device has removable storage – first check for encryption and unencrypt if so – then remove the removable storage prior to sanitization)**	
Apple iPhone and iPad (current generation and future iPhones and iPads)	
Clear:	Select the full sanitize option (typically in the 'Settings > General > Reset > Erase All Content and Settings' menu). (The sanitization operation should take only minutes as Cryptographic Erase is supported. This assumes that encryption is on and that all data has been encrypted.) Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	Select the full sanitize option (typically in the 'Settings > General > Reset > Erase All Content and Settings' menu). (The sanitization operation should take only minutes with Cryptographic Erase being supported. This assumes that encryption is on and that all data has been encrypted.)
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Before sanitizing the device, ensure that the data is backed up to a safe place. Current iPhones have hardware encryption – turned on by default.
Blackberry (back up data on device before sanitization)	
Clear:	BB OS 7.x/6.x - Select Options > Security Options > Security Wipe , making sure to select all subcategories of data types for sanitization. Then type "blackberry" in the text field, then click on "Wipe" ("Wipe Data" in BB OS 6.x) BB OS 10.x (Decrypt media card before continuing) Select Settings, Security and Privacy, Security Wipe . Type "blackberry" in the text field, then click on "Delete Data". The sanitization operation may take as long as several hours depending on the media size. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.

Purge:	BB OS 7.x/6.x - Select Options > Security > Security Wipe, then make sure to select all subcategories of data types for sanitization. Then type "blackberry" in the text field, then click on "Wipe" ("Wipe Data" in BB OS 6.x). For BB OS 10.x Select Settings> Security and Privacy>Security Wipe. Type "blackberry" in the text field, then click on "Delete Data". The
	sanitization operation may take as long as several hours depending on the media size.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Centralized management (BES) allows for device encryption. Refer to the manufacturer for additional information on the proper sanitization procedure, and for details about implementation differences between device versions and OS versions. Proper initial configuration using guides such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible. If the device contains removable storage media, ensure that the media is sanitized using appropriate mediadependent procedures.
Devices running the Google Android OS (connect to power before starting encryption)	
Clear:	Perform a factory reset through the device's settings menu. For example, on Samsung Galaxy S5 running Android 4.4.2, select settings, then, under User and Backup, select Backup and reset, then select Factory data reset. For other versions of Android and other mobile phone devices, refer to the user manual. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	The capabilities of Android devices are determined by device manufacturers and service providers. As such, the level of assurance provided by the factory data reset option may depend on architectural and implementation details of a particular device. Devices seeking to use a factory data reset to purge media should use the eMMC Secure Erase or Secure Trim command, or some other equivalent method (which may depend on the device's storage media). Some versions of Android support encryption, and may support Cryptographic Erase. Refer to the device manufacturer (or service provider, if applicable) to identify whether the device has a Purge capability that applies media-dependent sanitization techniques or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.

Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Proper initial configuration using guides such as the DISA STIGs (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible. Following the Clear or (if applicable) Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. When in doubt, check device manual or call tech support. For both Clear and Purge, refer to the manufacturer for additional information on the proper sanitization procedure.
Windows Phone OS 7.1/8/8.x (Centralized management may be needed for encryption)	
Clear:	Select the Settings option (little gear symbol) from the live tile or from the app list. On the "Settings" page, scroll to the bottom of the page and select the "About" button. In the about page, there will be a **reset your phone** button at the bottom of the page. Click on this button to continue. Choose Yes when you see the warning messages. Please note that after the process is completed, all your personal content will disappear. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	The capabilities of Windows Phone devices are determined by device manufacturers and service providers. As such, the level of assurance provided by the factory data reset
	option may depend on architectural and implementation details of a particular device. Devices seeking to use a factory data reset to purge media should use the eMMC Secure Erase or Secure Trim command, or some other equivalent method (which may depend on the device's storage media). In some environments, Windows Phone devices may support encryption, and may support Cryptographic Erase. Refer to the device manufacturer (or service provider, if applicable) to identify whether the device has a Purge capability that applies media-dependent sanitization techniques or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Before sanitizing your device, ensure that you back up your data to a safe location. Refer to the manufacturer for proper sanitization procedure, and for details about implementation differences between device versions and OS versions. Proper initial configuration using guides such as the DISA STIGs (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible.

All other mobile devices *This includes cell phones, smart phones, PDAs, tablets, and other devices not covered in the preceding mobile categories.*	
Clear:	Manually delete all information, then perform a full manufacturer's reset to reset the mobile device to factory state. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	See Destroy. Many mobile devices only offer capabilities to Clear (and not Purge) the data contents. A mobile device may offer Purge capabilities, but these capabilities are specific to the hardware and software of the device and should be applied with caution. The device manufacturer should be referred to in order to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear or (if applicable) Purge operation, manually navigate to multiple areas of the device (such as call history, browser history, files, photos, etc.) to verify that no personal information has been retained on the device. For both Clear and (if applicable) Purge, refer to the manufacturer for proper sanitization procedure.

Table A-4: Equipment Sanitization

Equipment	
Office Equipment *This includes copy, print, fax, and multifunction machines*	
Clear:	Perform a full manufacturer's reset to reset the office equipment to its factory default settings.
Purge:	See Destroy. Most office equipment only offers capabilities to Clear (and not Purge) the data contents. Office equipment may offer Purge capabilities, but these capabilities are specific to the hardware and firmware of the device and should be applied with caution. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers. Office equipment may have removable storage media, and if so, media-dependent sanitization techniques may be applied to the associated storage device.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.