Electronic Media Sanitization

Identifier: Media Sanitization 001	
Revision Date: 6/15/2017	**Effective Date:** 7/1/2017
Approved by: BOR CIO	**Approved on date:** 6/20/2017

Table of Contents

1. Introduction

CSCU policy requires digital media and applicable devices that contain university owned data be sanitized prior to reassignment or disposal in order to ensure that sensitive data is not revealed to unauthorized or inappropriate parties. This standard provides a number of approved sanitization methods that require a reasonable amount of resources to be compliant with OPM Disposal of Digital Media (IT-SEC-16-02).

2. Purpose

The purpose of this standard is to specify the requirements for implementing and maintaining a storage device sanitization program. All storage devices will need to be sanitized prior to being removed from service or deployed to a user at a different Data Classification Level or when a storage device could contain licensed software or DCL1 through DCL3 data. For more information on Data Classification Levels please see the Data Classification Standard. Fiscal procedures found in CSUS disposal of surplus property must still be followed.

3. Scope

The standard applies to all storage devices in the CSCU system that could contain licensed software or DCL1 through DCL3 data.

4. Definitions

Definition

5. Standards

5.1 Digital Media Sanitization Methods

The computing environment is constantly moving forward with new technologies. While there are numerous ways in which data is stored, the methods of data disposal can be classified into one of three methods; Overwrite, Cryptographic Erase (CE), or Destroy. Media type and destination play an integral role in determining which method to use.

Magnetic tapes and Floppy Disks

Destination for Media / Device	Required
Transfer within University	Overwrite
Disposal / University Surplus	Destroy

Optical Disks (CD / DVD)

Destination for Media / Device	Required
Disposal / University Surplus	Destroy

Hard Drives

Destination for Media / Device	Required
Transfer within University	Overwrite or Cryptographic Erase
Disposal / University Surplus	Overwrite or Cryptographic Erase

Note: Destruction is required for damaged media when overwrite or CE cannot be completed.

Flash drives and Solid-state disk drives

Destination for Media / Device	Required
Transfer within University	Overwrite or Cryptographic Erase
Disposal / University Surplus	Overwrite or Cryptographic Erase

Note: Destruction is required for damaged media when overwrite or CE cannot be completed.

Mobile devices

Destination for Media / Device	Required
Transfer within University	Full hard-reset as specified by device manufacturer
Disposal / University Surplus	Full hard-reset as specified by device manufacturer

Copiers and Printers

Destination for Media / Device	Required
Transfer within University	Full hard-reset as specified by device manufacturer
Disposal / University Surplus	Full hard-reset as specified by device manufacturer

Networking Devices

Destination for Media / Device	Required
Transfer within University	Full hard-reset as specified by device manufacturer
Disposal / University Surplus	Full hard-reset as specified by device manufacturer

5.2 Overwriting Data

If media is transferred within the university, the drive format or drive repartition action that occurs during a computer reimage will suffice for Overwriting Data. Cryptographic erase on fully encrypted drives is the preferred method.

Hard Drives

In the case of overwriting Hard drives before surplus, overwriting once is considered sufficient to render them sanitized for transfer. Cryptographic erase on fully encrypted drives is the preferred method.

Flash Drives

In the case of overwriting flash drives before transfer or surplus, overwriting once is considered sufficient to render them sanitized for transfer.

5.3 Media/Device Destruction

Suitable methods of media/device destruction are as follows:

- Incineration - This method involves destruction of the device/media by burning. This will result in the information stored on the device being completely unrecoverable.
- Pulverization - This method involves mechanically reducing the device/media into small enough pieces to make recovery of data very difficult, if not impossible. This is typically done via a series of hydraulic or pneumatic impact devices.
- Shredding - This method destroys the device/media by cutting it into either strips or small chunks (in the case of cross-cut shredders). When shredding optical drives and floppy disks strip shredders are considered sufficient.
- Crushing - This method destroys the device (typically a hard drive) through the rapid application of a large amount of force to the media in question.

Degaussing

If the intention is to reuse the device/media after sanitization is completed, it is most prudent to perform the sanitization via overwriting, as detailed below. Degaussing must be performed using a degaussing unit before the storage device/unit is disposed of.

Cryptographic Erase

If full disk encryption is used, sanitization of the target data is reduced to sanitization of the encryption key(s) used to encrypt the target data. Thus, with Cryptographic Erase (CE), sanitization may be performed with high assurance and much faster than with other sanitization techniques. CE can also be used as a supplement or addition to other sanitization approaches.

Portable Devices (Mobile phone / Tablet)

Portable devices such as smartphones and tablets typically do not provide direct access to the device's storage, so they cannot be easily overwritten. To render these devices suitable for transfer/disposal, perform a full "hard" reset (i.e., a reset operation which erases all data and restores the devices to its factory defaults). If such a reset operation is not possible, all user data on the device must be manually deleted.

6. Compliance

Required Records

Records of data sanitization must be maintained in accordance with the state requirements set by the Office of Policy Management in the Disposal of Digital Media policy (IT-SEC-16-2) and the retention schedules set by Connecticut State Library (S6: Information Systems Records)

Data sanitization records shall include the following information:

- Media Type
- Serial Number (if applicable)
- Assigned property number (if applicable)
- Date of sanitization
- Method of sanitization
- Final disposition of media after data is sanitized
- Person performing data sanitization

7. Exceptions

To request an exception, please submit the Information Security Exception request to SecProg@ct.edu

The requestor and BOR Information Security Program Office will define the approved alternative configuration if different than the original proposal of the requestor.

The exception process is NOT an alternative to the Change Control Management process.

8. Related Publications

Related Policies

- BOR-Information Security Policy
- Disposition of Surplus Property Procedures Policy

Related Standards and Procedures

- Link to Support Services Procedure Page

Web Sites

- CT State Library - Records Retention Schedules for State Agencies http://ctstatelibrary.org/publicrecords/general-schedules-state
- OPM Disposal of Digital Media (IT-SEC-16-02) http://www.ct.gov/opm/lib/opm/secretary/disposal_of_digital_media_policy.pdf
- Office of State Comptroller http://www.osc.ct.gov/manuals/PropertyCntl/index.html http://www.osc.ct.gov/manuals/PropertyCntl/chapter09.htm
- NIST Special Publication 800-88 – Guidelines for Media Sanitization http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
- U. of Illinois Disposal of Digital Media Standard https://wiki.cites.illinois.edu/wiki/display/ITStandards/Disposal+of+Digital+Media+Standard

9. Revision History

Previous versions of this standard

- None

History of Changes

- None

Standards superseded by this standard

- Modifies the CSUS media destruction requirements in Section C of CSUS Procedures for the Disposal of Surplus Property