The University of Texas at El Paso
Electronic Data Destruction Guidelines

Contents

Introduction

The University of Texas at El Paso Information Security Office (ISO) shall provide guidelines for describing the required steps for protecting and disposing of electronic media, in this case disks, tapes, hard drives, etc., containing electronic Confidential or Controlled university data (formerly known as Category I data) in a manner that adequately protects the confidentiality of the Data and renders it unrecoverable.

For any questions or concerns regarding any of the material in this document, please contact the Information Security Office.

Purpose

This guideline provides approved methods for overwriting or modifying the electronic media to make it unreadable or indecipherable or otherwise physically destroying the electronic media. For additional information, please refer to The University of Texas at El Paso Information Security Policy and associated Standards (e.g., Standard 11: Data Classification Standard), UTEP Records Retention Schedule, and the UTS165 Information Resources Use and Security Policy.

Scope

These guidelines apply to Data Owners and Custodians, who must maintain an inventory and have documentation of all systems that house Confidential or Controlled University Data, as well as Technology Implementation Managers (TIMs), Technology Support, Telecommunications Infrastructure, Enterprise Computing, Surplus, the ISO, and others as required.

Procedures

- **Begin the Process**
    - Departments / Colleges must create a Service Now Request by composing an email to helpdesk@utep.edu *or* by emailing security@utep.edu prior to contacting Surplus for destruction or pick-up of electronic devices. A Service Now request will automatically be generated from the email request. ***Any machine containing Controlled Unclassified Information (CUI) will need to be handled directly by the Information Security office, which can be reached at security@utep.edu.***
    - Provide the following information when you **create a ServiceNow Request *or* email ISO**:
        1. **SUBJECT LINE**: "Device Destruction – (Department)"
        2. **BODY**:
            - **Department*:***
            - **Point of Contact**:
            - **Extension/Phone**:
            - **Building, Room Number**:
            - **Description of Device**: *(e.g., hard drive, tape, HD from server; brand/model may be helpful here)*
            - **UTEP Inventory Tag Number of Device** (if applicable):
            - **Serial Number**:
            - **Hard Drive Make/Model**: *optional, but appreciated*
            - **Hard Drive Serial Number**: *optional, but appreciated*

        - You may use the following Command Prompt to retrieve hard drive information:

          `<wmic diskdrive get model,serialNumber`
    - **Disposition is for** (if applicable):
        - *Surplus*
        - *Reuse*
        - *Other* (**Specify**):

- **Device Destruction Methodology**
    - The data will be destroyed by the Technology Support Team by writing two initial passes of random data on the device following by a final pass of zeros.
    - **NOTE**: All CUI devices are handled by ISO, and all CUI labels should be removed from sanitized systems.
    - The following programs are approved by the ISO for performing electronic data "erasure". Use of other destruction methods requires CISO approval.

        1. ***Securely Erasing an SSD with Bitlocker on Windows, on a live system for decommission or an external/secondary drive***
            - Open the Control Panel, navigate to "System and Security," and choose "Manage Bitlocker" (or search for Bitlocker on the Start Menu)
            - For the SSD media that needs to be securely erased, choose "Turn on BitLocker" and follow the prompts.
                - Preferably, encrypt the device using a password. Use a long, randomly generated password and discard it after encrypting the drive.
                - Do not re-use encryption passwords for multiple devices or keep an association between a password and a drive if encryption is being used for secure wiping.
            - When asked, choose to encrypt the entire device.
                - **For secondary drives**
                    - After the disk is encrypted, you can format the disk from "This PC" or Disk Management.
                    - Formatting the disk will remove the Bitlocker encryption.
                    - If the keys were saved, delete them. Any data remaining on the disk from before the format should be encrypted, and without the key, irrecoverable.
                    - The secondary drive can be removed if necessary.
                - **For system drives**
                    - Using external media, delete all the partitions/format the system drive.
                    - The encryption keys will be deleted through this process, and the data will be unrecoverable.
            - **NOTE:** Systems encrypted using BitLocker, the TPM on the device will need to be cleared once the drive is wiped otherwise you will not be able to encrypt the data again with a new installation.

        2. ***Securely Erasing an SSD with FileVault on MacOS***

1. Open System Preferences, navigate to Security & Privacy, and choose the FileVault tab.
2. Turn on FileVault for the boot drive, then create and retain a recovery key for later.
3. When the SSD is fully encrypted, reboot the Mac into Recovery mode (? + R during boot)
4. From Recovery mode, launch Disk Utility. Select your encrypted boot SSD and choose "Unlock [volume name]" from the File menu and provide the recovery key from step 2.
5. When the disk is unlocked, erase the disk in Disk Utility. This will remove the encryption key and data on the disk, making everything on the disk unrecoverable.
6. If required, reinstall MacOS if the device is to be reused.

3. ***Prepare the Bootable drive and execute Darik's Boot and Nuke (DBAN) - http://www.dban.org/***
    - The DBAN iso has been added to the KACE environment, which allows for wiping of drives via PXE boot. When you perform a PXE boot, the DBAN disk will show up as an option under the KACE boot menu. You will be required to logon with a password to access this feature.
    - **NOTE**: DBAN will **not** work on Solid State Drives (SSDs) or RAID – For these types of drives it is recommended to use one of the other methodologies listed below.

4. ***Prepare a Bootable USB with a Linux image, access the Boot menu on the device, and Boot from USB to then use scripts in Terminal***
    - Use *'fdisk'* to list all drives and -l to include their corresponding names.
        - `>sudo fdisk -l`
    - The *'hdparm'* command can be used to inspect the Hard Disk, using Any Linux Distribution; this is used to gather the information on the drive for documentation and proper identification.
        - `>sudo hdparm -I /dev/<drive>`
        - <drive> is usually sda or sdb use.
    - Select the viable option for erasing from the following options:
        - Using **HDPARM**; which is best for fast, secure full-drive erasure (especially SSDs via firmware)
            - `>sudo hdparm --user-master u --security-set-pass PASSWORD /dev/<drive>`
                - A temporary password is required before the erase command can be issued.
            - `>sudo hdparm --user-master u --security-erase PASSWORD /dev/<drive>`
                - Issue the Secure Erase command, which may take from a few minutes for SSD to several hours for a large HDD.
            - `>sudo hdparm -I /dev/<drive>`

        - Verify completion; the output should show “not enabled,” which means the security password has been automatically cleared.
    - Using **Shred**, used for deleting sensitive files on HDDs, and is available on any Bootable Linux Distribution.
        - `>sudo shred -vf -n 2 -z /dev/<drive>`
            - -v = verbrose, will display progress.
            - -f =changes permissions to allow writing if necessary.
            - -n = define number of passes (best balance of security + time), default is 3.
    - Using **Scrub**, like Shred but more rigorous, and is available on any Linux Distribution.
        - `>sudo scrub -p dod /dev/<drive>`

5. ***Self-Encrypting Drives (SEDs)***
    - For SEDs that are encrypted with SecureDoc, first use the SecureDoc Recovery Tool ‘PSID-Revert’ feature to revert to the default factory encryption key, then use the ‘Crypto Erase’ feature. This process may also be performed on Seagate drives by using the SeaTools ‘SED Crypto Erase’ feature.

6. ***SDELETE for select data***
    - Under circumstances where sensitive data needs to be cleared the Windows tool **SDELETE** can be used to ensure that the file has been fully deleted from memory (i.e., single file, folder, drive.).
    - **SDELETE**, part of Microsoft Sysinternal tools, is available for download: https://learn.microsoft.com/en-us/sysinternals/downloads/sdelete
    - Once downloaded, open Command Prompt as an Administrator and run the following command:
        - `>sdelete64.exe -c -p 5 <FULL PATH TO SPECIFIED DATA>`
            - -p # = define number of overwrite pass (best balance of security + time). If not defined, the default number is 1 but 3 passes is recommended and no more than 5.
            - -r = recurse into files.
            - -s = process subdirectories even if they contain only folders.
            - -q = quiet mode, which is not recommended so progress can be seen.

7. ***Devices Not Erasable***
    - Devices that cannot be scrubbed due to damage, etc. must be physically destroyed; to include a punch tool, physically shredding, etc.). Arrangements must be made through the ISO for destruction of these types of devices.

        - If a device that handles **CUI** is **not** erasable, our recommendation is to have the drive **destroyed**, not repurposed.

- **Contact Surplus**
    - If the device is planned for surplus, the Surplus department may be contacted to pick-up the item.

- **Physical Destruction of Devices**
    - If required, the Surplus Department will physical punch devices as necessary.

- **Reuse of Devices**
    - Surplus will contact PC Support to pick-up any devices that have been appropriately erased for reuse.

- **Routers and Switches**
    - A RESET to the device's base configuration will be performed for all routers and switches being surrendered to the Surplus Department.

- **Destruction Validation**
    - Surplus will conduct a random check of devices certified as destroyed.

References

NIST Special Publication 800-88: Guidelines for Media Sanitization
UTEP Information Resources Use and Security Policy
UTEP Purchasing & General Services – Records Management
UTS165 Information Resources Use and Security Policy

Revision History

Date	Amendment Reason	Approved By
December 5, 2016	Creation of document.	Gerard D. Cochrane Jr. Chief Information Security Officer (CISO)
February 8, 2017	Incorporate additional requirements.	Gerard D. Cochrane Jr. Chief Information Security Officer (CISO)
May 9, 2017	Update approved destruction programs and add TS Certificate Label.	Gerard D. Cochrane Jr. Chief Information Security Officer (CISO)
March 8, 2024	CUI Consideration.	Gerard D. Cochrane Jr. Chief Information Security Officer (CISO)
May 8, 2026	Update to address labels.	Gerard D. Cochrane Jr. Chief Information Security Officer (CISO)