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 university data (formerly known as Category I data) in a manner that adequately protects the confidentiality of the Data and renders it unrecoverable.

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 University Data, as well as Technology Implementation Managers (TIMs), Technology Support, Telecommunications Infrastructure, Enterprise Computing, Surplus, the ISO, and others as required.

Procedures

1. Begin the Process - Departments / Colleges must create a Service Desk 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 Desk Request will be automatically 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.***

2. Compose the Email - When composing the email request it should contain the following:
   SUBJECT LINE: "Device Destruction – (Department)"; where department is listed.
   BODY: Include the following information in the body of the email request
   a. **Department:**
   b. **Point of Contact:**
   c. **Extension/Phone:**
   d. **Description of Device: (e.g., hard drive, tape, HD from server)**
   e. **UTEP Inventory Tag Number of Device (if applicable):**
   f. **Serial Number:**
   g. **Hard Drive Make/Model:**
   h. **Hard Drive Serial Number:**
   i. **Disposition is for (if applicable):**
      - **Surplus**
      - **Reuse**
      - **Other (Specify):**

   NOTE: Surplus will not pick-up any device until these guidelines have been adhered to.

3. Device Destruction Methodology – The Data will be destroyed by the Technology Support Team by writing two initial passes of random data on the device followed by a final pass of zeros. NOTE: Hard Drives that are encrypted may need to be first decrypted and/or unlocked and then overwritten. The following programs are approved by the ISO for performing electronic data "erasure". Use of other destruction methods required CISO approval.
   a. 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 1**: 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.
      - **NOTE 2**: DBAN will not work on Solid State Drives (SSDs) or RAID – For these type of drives it is recommended to use one of the other methodologies listed below.
   b. 'hdparm' Command, to Inspect the Hard Disk, Using Any Linux Distribution

      >**sudo hdparm -i /dev/<drive>**

      <drive> is usually sda or sdb use **sudo fdisk -l** to list all drives and their corresponding names.
   c. 'Shred' Command Using Any Bootable Linux Distribution (e.g., Ubuntu, Mint, Caine, etc)

      >**sudo shred –vf –n 2 –z /dev/<drive>**

      <drive> is usually sda or sdb use **sudo fdisk –l** to list all drives and their corresponding names.
   d. 'Scrub' Program – Available from any Linux Distribution

      >scrub –p dod /dev/<drive>

      <drive> is usually sda or sdb use **sudo fdisk -1** to list all drives and their corresponding names.
   e. Self Encrypting Drives (SEDs)
      IMPORTANT: For SEDs that are encrypted with SecureDoc, first use the SecureDoc Recovery Tool 'PSID-Revert' feature to revert back 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.

4. Devices Not Erasable – Devices that cannot be scrubbed (i.e., potentially due to damage or because they came from a server, tape drive, etc.) must be physically destroyed. This process may include a punch tool, physically shredding, magnetic erasure, etc. Arrangements must be made through the ISO for destruction of these types of devices.

5. Label Device (usually desktop, laptop, server, etc.) – Only authorized personnel who have undergone ISO training may perform the device erasures. Likewise, only authorized personnel may create and affix a label on devices that have been appropriately erased. As a minimum, the labels must contain a signature line and printed name of the person who performed the erasure as well as a "Destroyed On" date. Please contact the ISO for labels.

OR


OR


6. Contact Surplus – If the device will be surplused, the Surplus department may be contacted to pick-up the item(s).
   NOTE: Surplus will not pick-up the device(s) unless the label has been affixed and contains the required information.

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

8. Reuse of Devices – Surplus will contact PC Support to pick-up any devices that have been appropriately erased (i.e., contain destruction label) for reuse.
9. 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. A destruction label will be affixed to the device containing the required information.

10. 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

Created:	December 5, 2016
Revised:	February 8, 2017 (incorporate additional requirements)
Revised:	May 9, 2017 (update approved destruction programs and add TS Certificate Label)
Revised	March 8, 2024 (CUI Consideration)
Approved:	December 5, 2016 Gerard D. Cochrane Jr., CISO
Approved:	May 9, 2017 Gerard D. Cochrane Jr. Chief Information Security Officer