Creighton
UNIVERSITY

Standard

DEPARTMENT: **Information Technology**	Revision:1 Date: 3/13/13
PROCEDURE: **Data Destruction Standard**	PAGE **1** OF **3**

PURPOSE

The purpose of this standard is to provide specific steps for secure destruction of Creighton data.

SCOPE

This document describes the steps necessary to destroy data or media in a secure manner.

STANDARDS

When University data is no longer needed it should be disposed of in a secure and responsible manner.

Paper Records

Confidential Data must be destroyed by one of the following methods:

- Cross-cut shredded to a particle size no larger than 4 x 30mm.
- Burned in a licensed incinerator.

Private Data must be destroyed by one of the following methods:

- Cross-cut shredded to a particle size no larger than 8 x 40mm.
- Burned in a licensed incinerator.

Public Data may be discarded by the following method:

- Recycled or disposed of in the trash.

Magnetic Media (ie floppy disks, hard drives, tape drives, etc)

Confidential Data must be destroyed by one of the following methods:

- If the media is going to be reused or redeployed within the University the media must be overwritten with random data using a tool approved by the Information Security Office.
- If the media is going to be disposed of or recycled, one of the following methods must be followed:
  - Physically destroy floppy disks and tape drives by shredding the platters or tape by cross-cut shredder into particles no larger than 4 x 30mm
  - Physically destroy magnetic media through pulverizing or crushing by a device or vendor approved by the Information Security Office.
- If the media is going to be returned to the vendor, one of the following methods must be followed:
  - Media must be overwritten with random data using a tool approved by the Information Security Office.
  - A contract with the vendor that states the vendor will securely wipe the media prior to reuse or disposal.

Private Data must be destroyed by one of the following methods:

- If the media is going to be reused or redeployed within the University the media must be overwritten with random data using a tool approved by the Information Security Office.
- If the media is going to be disposed of or recycled, one of the following methods must be followed:
  - Physically destroy floppy disks and tape drives by shredding the platters or tape by cross-cut shredder into particles no larger than 8 x 40mm
  - Physically destroy magnetic media through pulverizing or crushing by a device or vendor approved by the Information Security Office.
- If the media is going to be returned to the vendor, one of the following methods must be followed:
  - Media must be overwritten with random data using a tool approved by the Information Security Office.
  - A contract with the vendor that states the vendor will securely wipe the media prior to reuse or disposal.

Public Data may be discarded by the following method:

- Recycled or disposed of in accordance with University Facilities Management Policies.

Optical Media (ie CDs, DVDs, etc)

Confidential Data must be destroyed by the following method:

- Physically destroy media by shredding, grinding, or incineration by a device or vendor approved by the Information Security Office.

Private Data must be destroyed by the following method:

- Physically destroy media by shredding, grinding, or incineration by a device or vendor approved by the Information Security Office.

Public Data may be discarded by the following method:

- Recycled or disposed of in accordance with University Facilities Management Policies.

USB removable media without hard drives (i.e. thumb drives, memory sticks, etc.)

Confidential Data must be destroyed by the following method:

- Physically destroy media by shredding, disintegrate, or pulverize by a device or vendor approved by the Information Security Office.

Private Data must be destroyed by one of the following methods:

- Physically destroy media by shredding, disintegrate, or pulverize by a device or vendor approved by the Information Security Office.
- Securely wiped using software approved by the Information Security Office.

Public Data may be discarded by the following method:

- Recycled or disposed of in accordance with University Facilities Management Policies.

Cell phones and other mobile devices must be destroyed by the following method:

- Manually delete all data such as call logs, phone numbers, applications, account information, etc. and then reset the device to factory defaults.

DEFINITIONS

CD - Compact Disc: a class of media on which data are recorded by optical means.

Destruction - The result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive.

Disintegration - A physically destructive method of sanitizing media; the act of separating into component parts.

Disposal - The act of discarding media with no other sanitization considerations. This is most often done by paper recycling containing non-confidential information but may also include other media.

DVD - Digital Video Disc: a disc the same shape and size as a CD; but the DVD has a higher density and gives the option for data to be double-sided or double-layered.

Hard Disk - A rigid magnetic disk fixed permanently within a drive unit and used for storing data.

Incineration - A physically destructive method of sanitizing media; the act of burning completely to ashes.

Media - Material on which data are or may be recorded, such as paper, punched cards, magnetic tape, magnetic disks (hard drives, floppy disks, etc.), solid state devices (USB thumb drives), or optical discs (CDs, DVDs, etc.).

Optical Disks - A plastic disk that is “written” (encoded) and “read” using an optical laser device. The disc contains a highly reflective metal and uses bits to represent data by containing areas that reduce the effect of reflection when illuminated with a narrow-beam source, such as a laser diode.

Overwrite - Writing patterns of data on top of the data stored on a magnetic medium as a means of rendering the original data irretrievable.

Pulverization - A physically destructive method of sanitizing media; the act of grinding to a powder or dust.

Shred - A method of sanitizing media; the act of cutting or tearing into small particles.

Wipe - Process to remove information from media such that data recovery is not possible.

AMENDMENT/TERMINATION OF THIS STANDARD

The University reserves the right to modify, amend, or terminate this standard at any time.