SPACE INSTITUTE
Information Technology

Data Destruction and Sanitization Procedure

Effective Policy Date: **May 30, 2023**

Purpose of document: **The document addresses the procedures and processes followed for Arizona Space Institute regarding IT Asset & Media Retirement.**

Office/department responsible: **Arizona Space Institute, Office of Information Technology**

Procedure Statement

ASI users may store sensitive information on computer hard drives and other forms of electronic media. As new equipment is obtained and older equipment and media reach the end of life, sensitive information on surplus equipment and media must be properly destroyed and otherwise made unreadable to protect Confidential & Regulated Information.

Reason for Procedure

This document provides the processes to be followed to 1) maintain the integrity of computer systems and university data by following proper data destruction and sanitation procedures, and 2) to establish a baseline methodology and guidelines for computer/media retirement.

Who Needs to Know This Policy?

All personel within the Arizona Space Institute, Office of Information Technology

Contacts

Responsible College Official: Tim Swindle - Director – Arizona Space Institute

Responsible College IT Official: Nicolas Altamirano - Director, Information Technology

Responsible University Office: Arizona Space Institute, Office of Information Technology

If you have any questions on the procedure, you may send an e-mail to ASI-IT@arizona.edu

Web Address for this Policy

https://it.space.arizona.edu/compliance/policy-procedure-guidance

Data Destruction and Sanitization Procedure

A. General

The transfer or disposition of data processing equipment, such as computers and related media, shall be controlled and managed according to NIST 800-171 guidelines. Data remains present on any type of storage device (whether fixed or removable) even after a disc is "formatted", power is removed, and the device is decommissioned. Simply deleting the data and formatting the disk does not prevent individuals from restoring data. Sanitization of the media removes information in such a way that data recovery using common techniques or analysis is greatly reduced or prevented.

B. DATA DISPOSAL PROCEDURES

All computer desktops, laptops, hard drives, and portable media must be processed through the Arizona Space Institute IT Department for proper disposal. Paper and hard copy records shall be disposed of in a secure manner as specified by the archiving and destruction policy. The IT Director shall ensure procedures exist and are followed that:

• Address the evaluation and final disposition of sensitive information, hardware, or electronic media regardless of media format or type.

• Specify a process for making sensitive information unusable and inaccessible. These procedures should specify the use of technology (e.g. software, special hardware, etc.) or physical destruction mechanisms to ensure sensitive information is unusable, inaccessible, and unable to be reconstructed.

• Authorize personnel to dispose of sensitive information or equipment. Such procedures may include shredding, incinerating, or pulp of hard copy materials so that sensitive information cannot be reconstructed. Approved disposal methods include:

- **Physical Print Media** shall be disposed of by one (or a combination) of the following methods:

- ***Shredding*** - Media shall be shredded using cross-cut shredders.
- ***Shredding Bins*** - Disposal shall be performed using locked bins located on-site using a licensed and bonded information disposal contractor.

- **Electronic Media** (physical disks, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard-drives, etc.) shall be disposed of by one or more of the following methods:
  - ***Overwriting Magnetic Media*** - Overwriting uses a program to write binary data sector by sector onto the media that requires sanitization.
  - ***Degaussing*** - Degaussing consists of using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state.
  - ***Physical Destruction*** – implies complete destruction of media by means of crushing or disassembling the asset and ensuring no data can be extracted or recreated.

  IT documentation, hardware, and storage that have been used to process, store, or transmit Confidential or Regulated Information shall not be released into general surplus until it has been sanitized and all stored information has been cleared using one of the above methods.

Procedure

a. Windows, Mac, and Physical Servers:

i. Remove Electronic Media from Device (Workstation or Server)

ii. Document the Computer Name the electronic media came out of

iii. If media is a spinning disk (HDD) place the drive in the degausser.

iv. Run media through the degausser.

1. If the media is a solid-state drive (SSD or NVME) destroy the media using one of the following methods:
   a. Overwrite/Wipe the Drive using certified Hardware Erasing Tool
   b. Remove media from the SSD case and cut the media in half.
   c. Puncture the drive by drilling multiple holes into the media.

NOTE:

If the electronic media is not removeable from the device i.e. Apple iMacs, iPads, Tablets, etc. ASI IT will perform the manufacturers recommended wipe process to remove existing data.

History/Revision Dates

Effective Date	Version #	Author	Description
May 30, 2023	1.0	Nic Altamirano	Initial version.

Next Review Date: 5/30/2024