SJSU Electronic Data Disposition Standard

Executive Summary

University data is at risk as long as it is persistently stored on electronic media. This means that data must be properly cared for during its entire lifecycle on campus, and properly disposed of prior to leaving campus. Electronic Data Disposition standard outlines the steps necessary for the proper storage, decommissioning, and destruction of electronic data. This standard applies to all electronic computing devices and storage media acquired by the University or its auxiliary organizations including devices purchased through auxiliary or research funding. A computing device is any electronic device capable of receiving and persistently storing direct user input including but not limited to workstations, servers, tablets, laptops, and smartphones. Storage media is defined as any device which can receive and persistently store electronic data including, but not limited to USB drives, external hard drives, internal hard drives, SSD's, DVD's, magnetic tapes, floppy disks, etc.

Information Security Standards

SJSU Electronic Data Disposition Standard

Standard #	IS-EDDS	Effective Date	11/10/2015	Email	security@sjsu.edu
Version	2.0	Contact	Mike Cook	Phone	408-924-1705

Revision History

Date	Action
11/20/2013	**Reviewed: IT Management Advisory Committee, CISC, ITS Security Team**
6/26/2013	**Draft Policy Released**
3/5/2015	**Policy Reviewed – Michael Cook**
11/10/2015	**Incorporated changes from campus constituents – Distributed to Campus.**

Table of Contents

Introduction and Purpose

University data is at risk as long as it is persistently stored on electronic media. This means that data must be properly cared for during its entire lifecycle on campus, and properly disposed of prior to leaving campus. This standard outlines the steps necessary for the proper storage, decommissioning, and destruction of electronic data.

Scope

This standard applies to all electronic computing devices and storage media acquired by the University or its auxiliary organizations including devices purchased through auxiliary or research funding. A computing device is any electronic device capable of receiving and persistently storing direct user input including but not limited to workstations, servers, tablets, laptops, and smartphones. Storage media is defined as any device which can receive and persistently store electronic data including, but not limited to USB drives, external hard drives, internal hard drives, SSD's, DVD's, magnetic tapes, floppy disks, etc.

Standard

Physical Placement

All computing devices and storage media containing confidential Level 1 or Level 2 data must be located in a space such that when unattended, one or more of the following controls are in place:

1. The device and/or media are protected by entry controls to ensure that only authorized personnel are allowed to access the space containing the device.
2. The device and/or media are secured in a controlled container.
3. The device and/or media are physically secured to permanent furniture or structures within the space.

Decommissioning and Data Disposition: Computing Devices

1. Computing devices must be removed from the campus network in a timely manner when no longer in use.
2. System and network administrators must be notified of the computing device removal to ensure appropriate configuration changes to those systems and networks are made.
3. Disposition of a computing device and/or data must adhere to university asset management procedures.
4. Data stored on devices must be:
    a. Rendered unreadable before leaving the possession of the university.
    b. Rendered unreadable before transfer to another organization, either internal or external to the university, and prior to being reused or repaired.
    c. Kept in a location limited to authorized personnel while waiting to be processed to render the storage media unreadable.

Tools and Services

It is the responsibility of each department to ensure that data is rendered unreadable as part of the decommissioning process. All computing devices used to store Level 1, Level 2, or Level 3 information and all storage media which was used to store Level 1 or Level 2 information must be rendered unreadable using one of the following methods:

1. Campus Physical Media Destruction Service

   a. IT Services shall accept delivery of equipment and dispose of data via a Physical Media Destruction service. Visit the Information Security Web Site for official procedures.
2. Software-based Department of Defense (DOD) approved "Disk-Wiping"
   *** Does not apply to Solid State Disk Drives (SSD) , SSD's must be physically destroyed ***
   a. Darik's Boot and Nuke (DBAN)
   b. KillDisk
   c. Apple Disk Utility
   d. Mobile Device "factory wipe" feature
   e. Any other software package approved by the DOD
3. Other
   a. Must be performed by a hard drive shredding company or process approved by the Information Security Officer.

Documentation

Electronic media which was used to store confidential Level 1 and Level 2 data shall require documentation upon destruction. Departments utilizing Disk Wiping techniques shall self-certify destruction of the data. IT Services shall retain certificates for of all hard drives destroyed by the campus Physical Media Destruction Service.

All departments shall create, or delegate creation to their IT support group, records containing:

- Manufacturer and serial number of device which was wiped (Hard Drive, USB Drive, tape, etc.)
- Tag, manufacturer, and serial number of the computer the device came from (where applicable)
- Date of destruction or delivery to IT Services
- Method of destruction (i.e IT Services, DBAN, KillDisk).

Data Disposition Standard Management

In accordance with CSU policies, the San José State Information Security Officer oversees an annual review of this Standard and communicates any changes or additions to appropriate SJSU stakeholders. The standard shall be updated as necessary to reflect changes in CSU policies, SJSU's academic, administrative, or technical environments, or applicable laws and regulations.

The standard may be augmented, but neither supplanted nor diminished, by additional policies and standards.