

# Cal Poly Campus “Desktop Security Initiative” Standards, Guidelines and Practices: Storage Media and Secure Data Disposal-Disk Wiping

---

## Introduction

Cal Poly’s Information Security Officer and Chief Information Officer jointly act to establish campus standards to protect University information as well as data and systems that support and enable its appropriate uses. These apply to all electronic devices connected to the University network including computers, network switches and routers, personal digital assistant devices, laptop computers, etc., in accordance with the "Responsible Use Policy," "Information Security Program," and other campus computing policies. Among the requirements set forth is the protection of University information against unauthorized use.

## Purpose of This Document

This document will guide a computer technician through the use of Cal Poly’s standardized tool and processes to securely wipe hard disks of computers that are being (1) surveyed for public auction, (2) disposed of (e.g. drive is too small, old, or no longer needed), (3) reassigned to other individuals on campus, or (4) transferred to another department on campus. This is necessary to reduce possibility of inappropriate exposure of data and unauthorized use.

## Framework

**POLICY** – Individual departments shall be fully responsible for ensuring storage media (e.g. hard drives) have been wiped or destroyed prior to asset disposition or internal reassignment.

**STANDARD** – Use of the following tools (or equivalent) provide an appropriate and uniform level of protection for campus information (multi-wipe passes to DOD 5220-22.M standard):

1. Tools:

Darik’s Boot and Nuke (DBAN), a freeware utility available at <http://dban.sourceforge.net/> (Windows)

OR

Apple Disk Utility at <http://docs.info.apple.com/article.html?artnum=107437>

(Apple 10.3 operating system or older)

<http://docs.info.apple.com/article.html?path=DiskUtility/10.5/en/duh1011.html>  
(Apple 10.4 operating system or newer).

2. Standard:

Department of Defense (DOD) 5220-22.M Short

See NISPOM (February 2006): <http://www.dss.mil/isp/odaa/nispom06.html>

Cal Poly departments must follow these standards to ensure that electronic storage media have been thoroughly wiped or destroyed prior to asset disposition or internal reassignment.

This standard must be applied to hard drives of computers being internally reassigned or transferred, surveyed for public auction, or otherwise disposed of by the department.

The method of destruction must be appropriate to the classification of the information and media. If there is any doubt or concern regarding confidentiality of data, the most secure methods available must be utilized as outlined in the related procedure.

---

Departments needing to dispose of outdated (e.g., un-mountable hard drives, tape backups, etc.) or removable storage media (e.g., CD-ROMs, floppy disks, zip disks, etc.) must utilize specialized services for which the University has established contracts. This includes on-site disposal by a fully bonded and licensed disposal service that physically grinds and destroys media.

**GUIDELINE** – The DOD 5220-22.M standard is highly recommended for computers that are frequently re-imaged in controlled environments, e.g. open access computing labs or laptop checkout centers.

**PROCEDURE** – Refer to step-by-step guides posted at the Cal Poly Security Information Security Web site at: [http://www.security.calpoly.edu/what\\_technical\\_support/index.html](http://www.security.calpoly.edu/what_technical_support/index.html).

### **Contact Information**

Contact ITS Operations and Production Support at (805) 756-5512 for more information on specialized disposal methods.

Technical assistance is available by contacting the ITS Service Desk at 756-7000, who will route the call to the appropriate individual or team within User Support Services.

Contact [it-policy@calpoly.edu](mailto:it-policy@calpoly.edu) for clarifications regarding information technology security policies.