



IT Security Standard:

Media Disposal

Introduction

This standard defines the steps necessary to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding the disposal of computer system media. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines specific procedural and configuration elements for disposal of media used to store potentially sensitive data. This media may include magnetic, optical, and various printed media. For printed media such as paper, microfilm and fiche, this standard can be selectively applied to media specifically containing sensitive data. However, it does apply to all magnetic and optical media without exception.

For the purposes of the Bellevue College IT Security Standards, “sensitive data” includes, at a minimum:

1. All student and employee data.
2. All operational documentation and reports.
3. Any financial data containing institutional banking or personal data.

Exceptions

A variety of exceptions to this standard may be expected. These exceptions, when granted, will be documented in either a platform specific standard or in a memo documenting the exception. Exceptions may be granted by the Bellevue College IT Security Administrator, the Dean of Information Resources (IR), or any IR director authorized by the Dean. Copies of all documentation regarding exceptions will be kept on file with the Bellevue College IT Security Administrator. This documentation will include:

1. A detailed description of the exception.
2. A description of why the exception is necessary.
3. A risk assessment by the Bellevue College IT Security Administrator and/or the Dean of Information Resources, or designee.
4. A description of the compensating controls that are in place to mitigate risk created by the exception.

Business Impact and Risk, Threat and Vulnerability Analysis

The data resources within the scope of this standard are potentially data protected by one of a number of statutes, including the Health Information Portability and Accountability Act of 1996 (HIPAA) and the Family Education Rights and Privacy Act (FERPA). These laws, as well as other laws and policies, define a fairly high standard for protecting the confidentiality of student and employee personal data.

Given the sensitive nature of the data, the most significant threats are:

1. Accidental and/or malicious unauthorized access to sensitive data
2. Accidental and/or malicious destruction or disclosure of critical data

Given the nature of the asset and the nature of the threat, the primary risk associated with inadequate media disposal is litigation and loss of reputation for disclosing protected data for which Bellevue College is the custodian. There is also a risk of civil liability.

Standard

To ensure access to potentially sensitive data is not accidentally permitted, all computer system media will be disposed of following the procedures identified below.

A. Paper Reports and Microfiche

1. Printed material, paper, microfiche or microfilm containing sensitive data will be shredded prior to disposal. (Placing it in a locked shred barrel, for commercial shredding, is acceptable).

B. Removable Media (Floppy Disks, CDROM, Tape)

1. Removable media will be physically destroyed prior to disposal at its end-of-life.
 - a. 5-1/2 inch diskettes will be cut into at least four pieces.
 - b. 3-1/4 inch diskettes will be broken into at least 2 pieces.
 - c. CD ROM/DVD ROM will be broken in at least 2 pieces.
 - d. Magnetic Tape Cartridges will be broken, the tape will be pressed off its spool, and the tape cut somewhere well into the usable portion of the media.
 - e. Magnetic Reel Tape reels will be broken, the tape will be pressed off its spool, and the tape cut somewhere well into the usable portion of the media.

C. Hard Disk

1. All hard disks taken out of service for replacement or surplus will be either "scrubbed" or physically destroyed by IR technical support personnel.
 - a. Failed disks will not be returned to the vendor. These disks will either be drilled with at least three holes through the disk platters, or the platters will be destroyed (broken or bent) with a hammer.
 - b. Disks that have not failed, but are otherwise being disposed of, will be destroyed as described above or overwritten with, at minimum, five (5) passes of "zeroing" data. The actual data will include either random bits or alternating passes of all ones and all zeros.

D. Computer Systems

1. To ensure all computers are properly prepared for disposal, employees will contact Computing Services for assistance.
 - a. In addition to scrubbing the hard disk (as defined above), any computer system being taken out of service will be checked to assure there is no removable media (tapes, floppy disks, CDROM) left in the device.
 - b. Any Bellevue College documentation or labels, excluding state asset tags, will be removed.
 - c. A completed "Notice of Computer Equipment Storage Device Cleaning" form will be affixed to all surplus computing equipment.
2. Other computing devices with "permanent storage" will also be appropriately scrubbed of their stored data. At present, there are not many of these so they will be handled on a case-by-case basis, with procedures as approved by the Bellevue College IT Security Administrator and/or the Dean of Information Resources.

Sanctions

Violations of the provisions of this, or any Bellevue College IT security standard or policy, will be dealt with immediately in the same manner as any violations of Bellevue College policies, and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including:

1. Permanent loss of computer use privileges;
2. Denial of future access to Bellevue College IT resources;

3. Disciplinary action – any disciplinary action will be taken in accordance with appropriate procedures as established by the Vice President of Human Resources (for employees) or the Associate Dean of Student Success (for students);
4. Dismissal from the college; and/or
5. Legal action.

Those users who misuse or abuse any computing or network resource may have their login accounts closed and access to the systems immediately terminated. Some violations of this standard may also constitute a state, local, or federal criminal offense.

Appendix A – References

1. CIS IT Security Standard—*Media Disposal*, April 3, 2003
2. Bellevue College Policy # 4205: *Family Education Rights And Privacy Act: Disclosure Of Student Information*
3. Bellevue College Policy # 5250: *Information Technology (IT) Security*
4. Public Law 93-380, the Family Educational Rights and Privacy Act of 1974 (“FERPA”) <http://www.law.cornell.edu/uscode/20/1232g.html>
5. Health Information Portability and Accountability Act of 1996 (HIPAA) <http://aspe.hhs.gov/admsimp/pL104191.htm>

Effective Date:	July 2003
Date Last Modified:	April 12, 2009