



3000 Landerholm Circle SE • Bellevue, WA 98007-6484 • www.bellevuecollege.edu

IT Security Standard:

Portable Data Storage Devices

Introduction

This standard defines the specific steps needed to implement the Bellevue College IT Security Policy and other standards as they relate to the use of portable data storage devices connected to Bellevue College computers. This standard is necessary to help assure the integrity and reliability of the Bellevue College internal networks, the computers on those networks, and the software installed on those computers, and is meant to provide guidelines for the use of data storage devices, particularly those with large-capacity. The standard will be reviewed annually or when changes are implemented.

Scope

This document is intended to help define the acceptable use of data storage devices that can be connected to computers on the Bellevue College network, and to provide guidelines for educating employees about their additional responsibilities for security consciousness regarding the devices themselves and the data that may be stored on them.

This standard applies to all portable storage devices, whether owned by Bellevue College or by individuals, which are connected to the Bellevue College network and can be used to copy any kind of data or files from a Bellevue College-owned computer.

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

Data storage is an essential component in the use of computers—floppy drives and other storage devices have been a built-in part of computers since their inception. However, modern technology breakthroughs are changing the nature of the data storage capabilities of computers, impacting IT security.

Built-in storage devices are gaining capacity and it is not uncommon for rewritable CD-ROM disks or DVDs providing hundreds of megabytes of storage capacity to be used for everyday purposes by computer users. In addition, USB ports are now an ubiquitous hardware element in most computers, allowing for extreme flexibility in the connection of various portable devices to a modern computer.

A demand for increased flexibility and data storage capabilities led to development of large-capacity portable storage devices that are USB-compatible. In addition, some devices that are designed for other specific purposes can have a secondary capability of acting as a general data storage device (such as a

PDA or iPod). Many of these devices can be connected to a computer and configured in seconds, and some of these devices may have storage capacity that is actually larger than the hard drive of the computer to which they are connected.

The risk presented by these types of devices to the computing network and the data stored on it has led some organizations to ban them outright. However, such devices provide enormous flexibility in disaster recovery, in backing-up important data, and have legitimate business and educational functions, so their use at Bellevue College is permitted.

Inappropriate use of portable storage devices poses a number of risks:

1. Accidental or malicious disclosure of sensitive data to unauthorized parties
2. Theft, compromise or loss of protected, sensitive data
3. Accidental modification or destruction of data
4. Theft of computing components, such as software or portable devices
5. Loss of reputation

The direct physical risk to Bellevue College computers and networks presented by the use of portable storage devices is minimal. However, given the potential for theft or loss of data and/or software, theft or loss of the portable equipment, and the sensitive nature of the data stored on Bellevue College computers and networks, the use of portable storage devices at Bellevue College poses a severe risk for inappropriate or unlawful disclosure of data.

Standard

The use of portable data storage drives on Bellevue College-owned computers must always comply with all Bellevue College policies and IT Security standards, particularly those regarding access to and protection of data, software and equipment.

The key restrictions on portable data storage devices are related to two specific IT security principles. The first is concern for the physical protection of the device itself and the computer to which it is attached. The second principle is concerned with protection of Bellevue College-owned data and software, whether stored on the device or on the computer to which the device is attached.

For the purpose of this standard, portable data storage devices are defined to include any externally-connected computer hardware device capable of storing electronic files. These definitions include any hard drive, mp3 player, PDA or USB drive. In addition to the external nature of the device, a distinction must be made between two classes of portable data storage, based on their storage capabilities: large-capacity and small capacity.

Large-capacity portable data storage devices are defined by this standard as any external storage device with a capacity over 5 GB. Large-capacity portable storage devices will not be used at Bellevue College, except as allowed within the below sections of this standard.

Small-capacity portable data storage devices include any external storage device with a storage capacity below 5 GB. Small-capacity storage devices that are allowed include USB drives (also called thumb, key, stick, or pen drives). Small-capacity portable storage devices may be used provided no additional software aside from the operating system is required on the computer in order to make the drive work.

Internally-used devices

Though they can be strictly defined as “portable storage devices,” this standard does not govern the use of any floppy, Zip, CD-RW or DVD-RW disks that are inserted into internal computer drives. It does govern the connection of any external drive enabling such disks to be used.

Bellevue College-owned Devices

Large capacity portable data storage devices owned by Bellevue College may be used on Bellevue College computers just as any other hardware peripheral. However, in addition to the “Storage Limited to Data” described below, the following additional security requirements must be met:

1. **Single User**

- a. Portable data storage devices may be assigned to a single user who will bear responsibility for ensuring its use is compliant with Bellevue College policies and standards, just as with any Bellevue College-owned computer hardware.
- b. Because Bellevue College-owned portable storage devices can be moved on and off-campus, a Bellevue College Loan of State Equipment Form must be completed by the user and approved by the user's supervisor before it is given to the user or attached to a Bellevue College computer.
- c. The user must comply with the below listed responsibilities for Physical Security at all times.

2. **Multiple Users**

Generally, a portable data storage device is not intended to be shared, particularly if it is intended to be used both on and off-campus. In many cases, a campus user taking off-campus any data under the stewardship of another campus user is strictly against Bellevue College and Department of Information Services (DIS) policy, and may be a violation of state law. Therefore:

- a. No portable data storage device may be shared by multiple users unless the same users are sharing a single campus computer and it is connected to that computer.
- b. A portable data storage device shared by multiple users may not be taken off-campus or moved from the area of the computer to which it is intended to be connected.
- c. Any user of the computer to which the device is attached must comply with the below listed responsibilities for Physical Security at all times.

3. **Physical Security**

Bellevue College-owned portable storage devices must be kept physically secure at all times.

- a. If the device is permanently attached to the computer, a locking mechanism must be in place to prevent theft of the device.
- b. If the device is not permanently attached, it must be secured in a locked drawer, cabinet or space whenever the user is not physically present using the computer to which the device is attached.
- c. The device may not be loaned or given to any other individual without administrative approval.

Non-Bellevue College-owned Devices

1. Connection of a personally-owned, large capacity, portable data storage device to a computer on the Bellevue College network, either directly or through another hardware device, must be in compliance with the requirements identified in the Bellevue College IT security standard addressing "Connecting Non-Bellevue College Equipment to Bellevue College Networks":
 - a. A formal request must be made to Information Resources and approved by an authorized IR administrator using the "Non-Bellevue College Device Connection Form" appended to that standard.
 - b. All applicable standards regarding maintenance, security patches and software installations for the device will be followed.
2. If the device contains Bellevue College sensitive data (including passwords for Bellevue College-issued accounts, Bellevue College business documents, college data and student data), users will comply with the applicable expectations for physical security of the device described under "Physical Security," above, whether the portable data storage device is on or off-campus.
3. All processes and procedures required by the Bellevue College Software Licensing Compliance policy and the IT Security Standard addressing "Software Management" will be followed if personally-owned software is required to be installed to make the device operate correctly on the Bellevue College-owned computer.
4. **Storage Limited to Data**
 - a. Software applications will not be copied to or installed on any portable data storage device; only data may be stored on the device.
 - b. If the device is used for backup purposes, only data will be backed-up, not applications installed on the host computer.

- c. Whether the device is on or off-campus, any user of a portable data storage device which contains any sensitive or potentially sensitive Bellevue College data must take steps to ensure confidential Bellevue College information is not accidentally disclosed or stolen, and will comply with federal FERPA laws, state and local laws, and all Bellevue College privacy policies, procedures, and standards, including the Bellevue College IT security standard addressing the "Use of Bellevue College Resources Off-Campus."
 - d. Under no circumstances will either Bellevue College data or software be copied to any portable data storage device owned by a non-employee.
5. **Non-Employee Devices**
In addition to the requirements identified above, users who are not Bellevue College employees have additional requirements:
- a. Large-capacity, portable data storage devices which are connected to the Bellevue College network for use by visitors to the campus will only be used in electronic classrooms, labs and campus meeting spaces, and will only be allowed for the duration of the specific event requiring such access. In no other circumstances is connection of such devices allowed.
 - b. In accordance with the Bellevue College IT security standard addressing "Connecting Non-Bellevue College Equipment to Bellevue College Networks", such connectivity needed by visitors will be coordinated through the visitor's Bellevue College contact person.
 - c. Under no circumstances will any Bellevue College data or software be copied to a portable data storage device owned by a non-employee, except in the case of approved contractors/ vendors as allowed under the guidelines identified in the Bellevue College IT security standard addressing "Non-Employee Access to Bellevue College Systems and Data."
6. **Student Devices**
- a. Students will not connect large-capacity, portable data storage devices to a computer on the Bellevue College network unless required by an instructor for short-term use as part of curriculum requirements.
 - b. Such connections will only be allowed on a podium or presentation system in electronic classrooms, labs and campus meeting spaces, for the duration of the event. Use of such a storage device on a non-podium lab computer is prohibited.
 - c. Personally-owned software belonging to students is not allowed to be installed on any Bellevue College computer.

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 Dean of Student Services (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

- Information Technology (IT) Security Policy
- Bellevue College Acceptable Use of State Resources Policy
- Bellevue College Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems Policy
- Bellevue College Acceptable Use of Bellevue College Computers Policy
- Bellevue College Software Licensing Compliance Policy
- Bellevue College Access to Public Records Policy
- Bellevue College Federal Privacy Act Disclosure Policy
- Copyright and the Right of Fair Use Policy
- IT Security Standards:
 - Connecting Non-Bellevue College Equipment to Bellevue College Networks
 - Data and Program Backup
 - Data and Information Security
 - Database Management
 - External Data Transfer
 - Media Disposal
 - Non-Employee Access to Bellevue College Systems and Data
 - Physical Security
 - Software Management
 - Use of Bellevue College Resources Off-Campus

Effective Date:	June 2005
Date Last Modified:	July 10, 2009