

## *IT Security Standard:*

# **Portable Computer System Usage**

### **Introduction**

This standard defines the specific procedural and configuration elements in place to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding the management and use of Bellevue College-owned portable computer systems by college employees. This standard will be reviewed on an annual basis or when changes are implemented.

### **Scope**

This standard governs Bellevue College-owned portable computer systems used by Bellevue College staff for business purposes. Laptops and other devices that are connected to the Bellevue College network, but *not* owned by Bellevue College are not governed by this standard, but are expected to comply with the Bellevue College IT security standard addressing "Connecting Non-Bellevue College Equipment to the Bellevue College Network."

This standard addresses both portable computer systems that are assigned permanently to an individual as well as any Bellevue College-owned systems that are available for shared use. These shared computers fall into two categories: those systems which are part of the Information Resources equipment pool and those whose use is controlled by campus units. All of these categories of portable computer systems will comply with all Bellevue College policies and standards governing equipment usage. The use of any future portable computing device issued by the college which is capable of storing and transporting protected information should also conform to this standard.

### **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 computing resources within the scope of this standard are potentially critical infrastructure to the daily business and educational operations of Bellevue College, and represent a noteworthy security risk. In addition, the loss of any protected information stored even for a short while on these computers is a significant problem having considerable impact on the college. Therefore, the most significant threats related to utilization of portable computer systems are:

1. Theft or loss of computer equipment
2. Loss of sensitive or confidential data
3. Malicious and/or fraudulent unauthorized access to sensitive data

The most significant risk associated with the use of portable computer equipment is disclosure of stored protected information if the device is lost or stolen. This risk of theft is significant within the normal use of portable computer systems. If a user then chooses to copy sensitive or confidential data to a portable computer system, the vulnerability and risk increases, and if additional security measures are not in place to protect that data, the risk of disclosure is extremely high.

## Standard

### A. General

#### 1. Definitions:

- a. The term "protected information" is used to collectively indicate any information or data classified by the Bellevue College IT security standard addressing "Data and Information Security" as "sensitive", "confidential", or as "information requiring special handling."
  - b. Within this standard, the definition of "portable computer systems" includes "tablet"-type and hand-held computing devices, as well as traditional "laptop" computers.
2. An individual will be assigned personal responsibility for every portable computer system. Employees must complete and sign a "Portable Equipment Use Agreement" form, appended to this standard as Appendix B, when checking out such systems.
    - a. Copies of these and any other required documentation will be filed with the Bellevue College IT Security Administrator prior to the release of the system to the individual employee.
  3. Local accounts used to access any portable computer system will be configured only by Information Resources technical support personnel.
    - a. IR technical support personnel will ensure that any accounts created on any Bellevue College computer system are in compliance with Bellevue College policy #5150: Acceptable Use of Bellevue College Networks and Systems.
    - b. No individual without an IR-configured account may use any Bellevue College-owned portable computer system.
    - c. No other employee may add, delete, or otherwise modify any user account on the portable system, except to update his/her own user password.
  4. Information Resources technical support personnel will configure an encrypted file storage location for each individual user of any laptop computer used at Bellevue College.
    - a. IR technical support personnel will instruct the user taking responsibility for the computer that all documents are to be stored in that encrypted space.
    - b. Configuration and use of this storage space will be in compliance with the Bellevue College IT security standard addressing Encryption Tools and Protocols.
  5. If a portable computer system is used to transport protected information, the employee is required to take exceptional care to keep the data secure, just as if it were on campus, and will comply with all Bellevue College privacy policies, procedures, and standards.
  6. Bellevue College staff will also take great care at all times to prevent the loss or theft of any Bellevue College-owned portable computer system in their possession. Any use of portable computer systems will comply with the Bellevue College IT security standard addressing "Physical Security."
  7. A portable computer system may be configured by IR technical support personnel to access the Bellevue College networks through either wired or wireless means, as is appropriate based on the specific business use of the system.
  8. Bellevue College staff will ensure that Bellevue College-owned portable computer systems are not used by any individuals not already authorized to use Bellevue College computers or networks.

## **B. Individual Assignment of Portable Computer Systems**

1. Aside from complying with all the requirements described under “General” above, the assignment of a portable computer system to a single individual will generally follow the same requirements associated with assigning a desktop computer system.
2. In addition, an employee being individually assigned a portable computer system will also have elevated “administrative” privileges configured for their assigned computer.
  - a. The purpose in allowing users elevated rights on a portable computer system is to facilitate the use of the computer, including the ability for the user to set up networking connections for use while away from campus, and for the user to keep any operating system and antivirus files appropriately updated.
  - b. The assignment of any elevated privileges by IR technical support personnel to an individual will be in compliance with the Bellevue College IT security standard addressing Security Privileges.
  - c. Despite being assigned elevated privileges, no user may install software on any Bellevue College portable computer system in violation of Bellevue College Policy #5100: Software Licensing Compliance or the Bellevue College IT security standard addressing Software Management.
  - d. A user with elevated privileges may not remove, alter or reconfigure any IR-installed software on the portable computer system without permission from the Dean of Information Resources or appropriate designee.
3. Portable computer systems assigned on a permanent basis to individuals must be returned to the Help Desk on an annual basis so the operating system and antivirus files may be fully updated.
4. **Shared Use of Portable Computer Systems**
  - a. A portable computer system may be shared within a Bellevue College unit by multiple users. Any shared portable computer system must still comply with the requirements described in “General”, above. This particularly includes requirements for assignment of the computer to one individual who will be personally responsible for the system.
  - b. In addition, units may make their own procedures for keeping the computer physically secure and for access to it by authorized users.
  - c. **Creation of individual accounts on the shared computer by IR.**
    - i. In order to protect any data stored on the system by other users, no one using a system intended for shared use may be granted elevated user privileges.
    - ii. In addition, all shared portable computer systems must be returned to the Help Desk at least once every academic quarter to ensure that all applicable security and operating system updates are accomplished in a timely manner.

## **C. Bellevue College Laptop Pool**

1. Information Resources maintains a pool of laptops available to Bellevue College employees for check-out for business use. The procedures for use of these computers on each Bellevue College campus are different.
2. Reservations for a laptop must be made at least three (3) business days before the need through Request Center (<http://requestcenter.bellevuecollege.edu>).
3. **Main Campus**

All laptops available for check-out to staff or faculty will be managed as follows:

  - a. Security
    - i. Loaner laptops will be kept in a locked and secure facility within the appropriate IR area.

- ii. The use of these laptop computers must always comply with the requirements described in “*General*”, above.

b. Check-out procedures:

- i. The Bellevue College “Portable Equipment Use Agreement” form (Appendix B) will be used to document the check-out of a loaned laptop.
  - 1. The form will be read and signed by the user and approved by a unit administrator each time before a laptop is checked out.
  - 2. When a laptop is loaned out, it will be due back on the date identified on the form.
    - a. Exceptions are required for periods over 14 days, and will be granted with the permission of either the Dean of IR, the IT Security Administrator or IR designee delegated responsibility for the laptop pool.
  - 3. The user will receive a copy of the form for personal records.
    - a. The original of this form will be maintained on file in Information Resources. It will be used to inventory the laptop and all peripherals when the equipment is returned.
- ii. The employee will schedule an appointment with the Help Desk to pick up the laptop and plan to spend about 10-15 minutes to complete the check-out process.
- iii. The employee will be granted elevated privileges to the laptop, with rights as described in the Bellevue College IT security standard addressing Security Privileges.
  - 1. These privileges are being granted to facilitate the employee’s use of the laptop, so that installation and configuration of any ISP, personal e-mail or other software needed to perform work duties away from campus can be accomplished.
  - 2. Because these elevated privileges are temporarily granted only for the duration of the laptop loan, the employee does not need to obtain unit administrator permission to exercise these rights on a loaner laptop.
  - 3. The employee will comply with all other provisions of the Security Privileges standard.
  - 4. No software may be installed using elevated privileges in violation of Bellevue College Policy #5100: Software Licensing Compliance or the Bellevue College IT security standard addressing Software Management.
- iv. Portable computer systems loaned to employees will be configured by Information Resources to use the Bellevue College wireless network while on campus.
  - 1. If a user needs to physically connect the system through a wired network connection, the Help Desk should be notified so that an appropriate connection can be established.
  - 2. Once a portable computer system has been initially configured by IR, the user will be able to disconnect or reconnect to the network without further assistance.
- v. The employee will be notified that any data files created by the employee or copied to the laptop will be stored in the designated encrypted file storage folder. The employee checking out the laptop is responsible for removing any of their data files prior to returning the computer.
- vi. Individuals wishing to connect to any services through the Internet from off-campus must have their own personal Internet Service Provider (ISP) or dial-up account available.
  - 1. State law prevents IR technical support personnel from providing hands-on assistance in setting-up specialized non-Bellevue College software or networking access (such as ISP or dial-up).

c. Check-in procedures:

- i. When an employee checks in a laptop, they will be required to confirm on the "Portable Equipment Use Agreement" form (Appendix B) that all peripheral items checked-out with the laptop have been returned.
- ii. The IR staff member who receives the returned laptop will:
  1. Ensure that any program or data files stored on the laptop have been removed.
  2. Ensure that any configuration changes made by the employee while the laptop was loaned out are reset to original values.
  3. Remove any user profiles on the equipment.
  4. Run a virus scan and update the antivirus and operating system software (if applicable) before the laptop will be checked out again.

d. Maintenance

- i. Information Resources will review each laptop in the check-out pool at least quarterly. This review will include:
  1. Updating the operating system and ensuring that the appropriate system software patches are applied.
  2. Updating the antivirus software and running a virus scan.
  3. Checking the disk for previously missed user files that should be removed.
  4. Reviewing the configuration to assure any user changes have been reverted back to the Bellevue College standard image. This will be done by reduplicating the image from a standard image, if necessary. IR will maintain extra drives with a standard image to support this.

4. North Campus

The pool of loaner laptops available at North Campus will be managed in compliance with all of the requirements and procedures identified above. However, arrangements for the checkout of an available laptop may also be made with North Campus Information Resources staff in person or by phone (425-564-2236) at least three (3) business days in advance of the need.

## 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:

- Permanent loss of computer use privileges;
- Denial of future access to Bellevue College IT resources;
- 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);
- Dismissal from the college; and/or
- 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. SBCTC-IT IT Security Standard—Management of Laptop and Handheld Devices
2. Bellevue College Policy #5000: Acceptable Use of Bellevue College Computers
3. Bellevue College Policy #5100: Software Licensing Compliance

4. Bellevue College Policy # 5150: Acceptable Use of Bellevue College Networks and Systems
5. Bellevue College IT Security Standard: Connecting Non-Bellevue College Equipment to Bellevue College Networks
6. Bellevue College IT Security Standard: Data and Information Security
7. Bellevue College IT Security Standard: Security Privileges
8. Bellevue College IT Security Standard: Portable Data Storage Devices
9. Bellevue College IT Security Standard: Physical Security
10. Bellevue College IT Security Standard: Technology Purchasing and Logistics
11. Bellevue College IT Security Standard: Use of Bellevue College Resources Off-Campus

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