

IT Security Standard:

Technology Purchasing and Logistics

Introduction

This standard defines the specific requirements for implementing Bellevue College policy # 5250: Information Technology (IT) Security regarding the physical management of technology resources on campus. This standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard applies to all computing and computing-related technologies on campus, as defined within this standard, and to those individual campus users authorized to use those technologies. It is intended to specifically supplement state and Bellevue College administrative policies governing procurement and deployment of goods and services, which all continue to apply to the procedures and processes described here.

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 authorized 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 use of modern telecommunications technology to support business and educational operations is a crucial element in the success of the college. While deliberate attacks against the network and the data it protects are the college's primary security concern, the complex infrastructure and large number of individual networking components being used on campus creates risk for unexpected, unintentional results if the acquisition and deployment of technology components are not carefully governed.

Failure to carefully control the technologies which use the existing internetworking components, or those which, by attaching, become a component of the network, puts the daily business and operations of Bellevue College at risk. There are a large number of potential points of entry to the network, each a potential launching point for attacks on or failure of the system. If this were to occur, critical Bellevue College business (administrative, instructional, and public service) functions could be disrupted.

Given the high level of dependence on the network, the most significant threats are similar to those related to the failure of any network component:

1. Malicious and/or accidental damage to equipment or resources
2. Malicious and/or accidental denial/loss of service
3. Malicious and/or unauthorized access to or modification of data
4. Malicious and/or accidental modification of networking components

In assessing the nature of the asset and the nature of the threat, the primary risk associated with failure to appropriately manage the acquisition and deployment of technology on campus is loss of access to the technology—essentially a loss of service. This loss of service could have associated risks of: loss of revenue, dissatisfaction of those to whom Bellevue College provides services, interruption of productive work, and a loss of reputation.

Secondary to this threat is the potential for inappropriate use of the resources, including violations of state and/or federal law and policies, excessive bandwidth use, uses inconsistent with the Bellevue College mission, or uses that are in violation of the Bellevue College Acceptable Use policies.

Standard

A. Introduction

1. Information Resources has the primary responsibility for the acquisition, distribution and support of technology resources on campus. This requirement is designed to ensure interoperability between technology resources deployed on campus, to save campus units money when purchasing resources, and to encourage consultation with technically knowledgeable support personnel.
2. The determining factor regarding IR oversight for a specific type of technical resource is whether that technology attaches directly to a Bellevue College computer, to the Bellevue College network (wired or wireless), or to any device attached to a computer or the network.
3. While not a comprehensive listing of the technologies that may fall under the IR purview, the technologies covered under this standard include, but are not limited to:
 - a. **Hardware**, such as desktop and laptop computers, portable computing devices, network servers, infrastructure, wiring and other components, such as switches and hubs;
 - b. **Software**, whether it is for a computer or for a peripherally-connected device;
 - c. **Telephones** and their supporting technologies;
 - d. **Computer peripherals**, such as printers, scanners, speakers, headphones, etc;
 - e. **Audio/video equipment**, including televisions, projectors, various playback equipment, etc.
4. Sometimes it may be difficult to determine whether a specific campus technology is supported by IR or whether this standard applies to its acquisition and deployment. When in doubt, campus users are urged to contact Request Center (<http://requestcenter.bellevuecollege.edu>) with questions.

B. Technology Purchasing

1. Acquisitions

- a. Acquiring technology for use on campus requires prior approval from the Dean of Information Resources or an authorized designee. For the purposes of this standard, “acquire” has its standard meaning, as well as denoting any purchase, donation or free distribution of technology. This requirement applies to:
 - i. Any request to acquire hardware that will be or may be directly or indirectly connected to the Bellevue College network.
 - ii. Any request to acquire software that will be installed on any computer that is connected to the Bellevue College network.
 - iii. Any request to acquire any software or hardware that depends on a connection to a second device which is then attached to the Bellevue College network.
 - iv. The purchase or contracting of any technical services or technical support external to Bellevue College, particularly that which will extend, change or reconfigure any element of the Bellevue College network (such as computers, network cabling, network ports, or access points, as well as those technologies described above).

- b. Responsibility for managing and coordinating technology acquisitions will be delegated to IR purchasing representatives as assigned by the Dean. When possible, IR purchasing representatives will take advantage of group prices, educational discounts, and combining individual campus purchases to achieve savings for all campus users.
- c. Requests for the acquisition of technology should be approved through campus supervisors before being submitted to Request Center.

2. Hardware

- a. Bellevue College will provide a standard set of telecommunications hardware sufficient for each campus user to accomplish their individual work tasks.
 - i. This will include computers, telephones and access to the Bellevue College network and the wider internet, if appropriate.
- b. Campus users wishing to upgrade, change, add to or enhance their telecommunications hardware should obtain supervisory permission and then submit a request through Request Center, providing contact and budget information.
 - i. These requests must be approved by the Dean of Information Resources or an authorized designee.

3. Software

- a. In accordance with the Bellevue College IT security standard addressing "Software Management", Bellevue College provides standard software tools to its employees.
 - i. This "standard image" will be the base software installation for all workstations.
- b. Any organizational unit on campus can order additional software needed for use in their own area or off-campus.
 - i. Usually this is an individual order for a specific user, but it can be multiple licenses for multiple users.
 - ii. This software will be purchased using a budget belonging to the organizational unit.
 - iii. All requests for acquiring software licenses of any type require prior approval from a unit supervisor and the Dean of Information Resources or an authorized designee.
- c. All requests for purchase and installation of software licenses for use on Bellevue College-owned computers and networking systems will be processed through Request Center.
- d. IR will process and install the software following the guidelines in the Bellevue College IT security standard addressing "Software Management."

4. Vendor Contracts

- a. Only those who have been authorized may install, configure or deploy technology on campus.
- b. IR technical support personnel must be involved prior to the event in the planning and execution of any technology installations or configurations requested by campus users performed by non-Bellevue College technical personnel.
- c. All vendor contracts providing technical equipment, services or support to any campus unit will be managed and approved in accordance with the "*Vendor*" section of the Bellevue College IT security standard addressing "Non-Employee Access to Bellevue College Systems" and the standard addressing "Technology Partnerships," whether they include an acquisition of new technology or not.

5. Reimbursements

- a. Many campus users have permission to purchase goods and services relevant to the business functions of the unit to which they are assigned. However, technology should not be purchased for use at Bellevue College without permission.

- i. Individuals will not be reimbursed for any technology acquisition that does not have approval from their supervisor and from an authorized Information Resources purchasing representative.

C. Technology Logistics

1. Logistics is defined as the method used to acquire, transport and store resources used by a business. By having efficient and proper logistical procedures, Bellevue College can cut costs and increase efficient use of the technology resources in place on campus. The procedures identified in this standard help ensure the continuing availability of installed technology components, while supporting innovation and keeping the technology at Bellevue College up-to-date and modern.

2. Installation and Maintenance of Technology

- a. No hardware or software on campus will be installed or set up as part of the Bellevue College network except by IR technical support personnel or authorized designees, no matter how it was acquired or who owns it. This includes any transfer of equipment or software between campus units or computers.
 - i. Campus users needing technology installed will submit a task to Request Center.
 - ii. This restriction does not apply to users setting up personally-owned laptop computers on the Bellevue College wireless network. Wireless users must comply with all procedures identified in the Bellevue College IT security standard addressing "Wireless Network Configuration and Management."
- b. Computers set up by IR technical support personnel will be configured and connected to the Bellevue College network following standard IT industry best practices.
- c. All networked Bellevue College computers will have a unique identifying name using a format which describes its location and primary user and any other distinguishing identifiers as directed by the Dean of Information Resources or authorized designee. Under no circumstances will a campus user change the network identifying name of a Bellevue College computer without authorization from the Dean of Information Resources.
- d. Software installations must meet the requirements of Bellevue College policy # 5100, "Software Licensing Compliance", and the Bellevue College IT security standard addressing "Software Management."
- e. Due to high maintenance costs and technician time, no campus user will be personally assigned more than two (2) computers without demonstrating a business need to do so and obtaining specific permission from their unit administrator.

3. Creation of Computer Labs or Electronic Classroom

- a. No computer lab or electronic classroom on campus will be established, moved, changed or expanded without the permission of the Dean of Information Resources or an authorized designee.
 - i. IR support personnel must assess the physical infrastructure supporting any such change. This includes switches and hubs supporting the network port capabilities of any space desired for a lab.
 - ii. Viable plans for on-going maintenance and support must be included in any decision to establish or expand a computer lab on campus, and must be approved by the Dean of Information Resources or an authorized designee.
- b. Creation of a new computer lab or electronic classroom may be initiated by submitting a task to Request Center.

4. Moving Technology Resources

- a. Because of the security measures in place to secure the Bellevue College network resources, physically connecting or disconnecting a component of the network, including

desktop computers, requires careful configuration of the component as well as the specific physical network port to which it is connected. Therefore:

- i. Information Resources technical support personnel are the only campus employees authorized to physically move Bellevue College technological resources from one location to another.
 - This includes the movement of resources within the same office space, as well as from location to location on campus.
 - Campus Operations personnel may assist in the moving of technology under the direction of the Dean of Information Resources or an authorized designee.
 - Campus users needing technology moved will submit a task to Request Center.
- ii. This requirement does not apply to technology or devices whose primary purpose is intended to be portable, such as laptop computers, portable drives or removable storage media.

5. Transfer of Technology Resources

a. Internal Bellevue College Computer Hardware Transfer

- i. If a computer is transferred to a user within the originating unit, all software licenses legitimately owned by Bellevue College and installed on the computer will remain with the computer.
- ii. If a computer is transferred to a user outside the originating unit, Information Resources will set up the transferred computer at the receiving location and reformat the computer as necessary.
 - All software necessary to meet the business needs of the recipient will be inventoried and reinstalled, as appropriate under the IT security standard addressing "Software Management" and the Bellevue College "Software Licensing Compliance" policy.

b. Internal Transfer of Rights to Bellevue College Software

- i. Software licenses not included in the campus standard software agreements can be transferred between Bellevue College units with the approval of the administrator of the program/department that originally purchased the software and the administrator of the program/department receiving the software.
 - The originating unit administrator will be responsible for requesting that Information Resources make such software transfers.
- ii. To ensure compliance with federal, state and local copyright laws and the IT security standard addressing "Software Management" and the Bellevue College "Software Licensing Compliance" policy, only authorized Information Resources support personnel will transfer software licenses and rights between departments and/or users.
 - Information Resources personnel will be responsible for updating the records of the distribution of the software.

6. Disposal of Computers and Technology Resources

- a. Bellevue College-owned technology resources capable of retaining digital copies of data, such as removable media, hard disks and computer systems must be disposed of in accordance with the Bellevue College IT security standard addressing "Media Disposal."
 - i. To ensure that all computers are properly prepared for disposal outside of Bellevue College, campus users will submit a task to Request Center when disposing of this type of equipment.
- b. All other Bellevue College-owned technology will be disposed of in accordance with state policies regarding state-owned equipment.

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. Bellevue College Policy #5000, *Acceptable Use of Bellevue College Computers*
2. Bellevue College Policy #5100, *Software Licensing Compliance*
3. Bellevue College Policy #5150, *Acceptable Use of Bellevue College Networks and Systems*
4. Bellevue College Policy #5250, *Information Technology (IT) Security*
5. Bellevue College Policy #5300, *Computer Labs*
6. Bellevue College IT Security Standard: *Media Disposal*
7. Bellevue College IT Security Standard: *Non-Employee Access to Bellevue College Systems and Data*
8. Bellevue College IT Security Standard: *Network Device Configuration*
9. Bellevue College IT Security Standard: *Physical Security*
10. Bellevue College IT Security Standard: *Software Management*
11. Bellevue College IT Security Standard: *Technology Partnerships*
12. Bellevue College IT Security Standard: *Wireless Network Configuration and Management*

Effective Date: May 2006
Date Last Modified: April 12, 2009