

## *IT Security Standard:*

# Physical Security

### Introduction

This standard defines the steps needed to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding physical security. The standard will be reviewed on an annual basis or when changes are implemented.

### Scope

This standard addresses the physical security of Bellevue College technology support and data processing facilities, including all the network server rooms, wiring closets, switch closets, and support, storage and office areas used by Information Resources (IR).

The computing labs on campus are special areas. They have both a high concentration of computers and fairly free access by students and campus visitors. As such, they present a different set of issues, most of which are addressed in Bellevue College policy # 5300: Computer Labs. From the perspective of physical security for these areas, the concern is to restrict access unless a Bellevue College staff member or faculty member is present to prevent theft or vandalism.

### 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

Physical security is the first line of defense in protecting the computer-based assets of Bellevue College. This is especially true of the administrative computer systems, but may include computer labs and classrooms as well, particularly because they may share a common physical infrastructure with the administrative systems. Because of the highly mobile nature of the campus population and the open public access to campus on a daily basis, physical security is of paramount concern.

Given the high level of dependence on computing technology for conducting the business of the college, the most significant threats are:

1. Malicious and/or unauthorized access to systems
2. Theft of computing or infrastructure components
3. Accidental and/or malicious physical damage to computing or infrastructure components
4. Accidental and/or malicious interruption to electrical power environment
5. Accidental and/or malicious interruptions to the necessary operating environment

Given the nature of the threat and history at Bellevue College, the greatest vulnerabilities are the environmental ones. The risk for those threats, however, is relatively low due to thoughtful planning and

learning from past incidents, and the business impact is likely to remain minimal. The next greatest vulnerability is likely to be accidental damage. With the controls in place to mitigate the threat, its overall risk is also fairly low. The strongest and most consistent threat continues to be security of physical assets and unauthorized access to systems. This could significantly impact the operations of the college.

## Standard

### **A. External Building Controls**

#### **1. Access Controls**

- a. The primary means of access control is through the use of traditional metal keys that are individually assigned to authorized Bellevue College employees.
- b. Coded key-pads will also be used to limit access to certain rooms and areas. Key code records will be maintained by Campus Operations.
- c. From time-to-time vendors, members of other state agencies/entities, or contractors will be issued metal keys in order to meet their specific access needs.
  - i. Before granting any special requests for key(s), Bellevue College management will evaluate the request for appropriateness.
  - ii. These non-Bellevue College entities will check out needed keys from Campus Operations/ Public Safety after obtaining appropriate approval.
  - iii. Keys will be issued in these circumstances only for the day and will be returned to Public Safety before the vendor leaves the campus.
- d. The entrances to labs, offices and classrooms will be accessible to authorized staff via key twenty-four hours a day, 365 days a year. Any electronic classroom and/or computer lab external doors will not be unlocked unless an authorized faculty or staff member is present in the room, or authorized by the Bellevue College IT Security Administrator and/or the Dean of Information Resources or authorized designee.
- e. Changes to business hours or access controls assigned to a key code will be made only with prior approval of the Dean of Information Resources or authorized designee.
- f. If a key is believed to be lost, it will be reported to the employee's supervisor immediately so doors that are accessed by that key can be re-keyed, if necessary.
- g. The back receiving doors for the IR work areas will remain locked at all times, except when receiving shipments or when the immediate area is occupied by authorized staff.
- h. Signs will be posted at or near the entrances to Restricted Access IT areas as defined below, and will be strictly enforced.
- i. It is not very difficult to subvert these security measures. Therefore, each employee also needs to take an active role in assuring the security of campus building:
  - i. Care will be taken to ensure that unauthorized people do not get access by "coat-tailing" or following in on an authorized person's access.
  - ii. Personally-assigned keys and key codes will not be loaned out to another person. If a loaner key is needed, one will be checked out from Campus Operations or an authorized designee.
  - iii. Employees are accountable for their visitors and guests while in secure areas.
  - iv. If an employee sees an unrecognized, unescorted person within a Restricted Access IT Area, that employee is responsible to either contact the Public Safety office (Ext. 2400) or ask for identification from the unknown person.

- v All IT staff will wear identification badges at all times.

## **B. Internal Building Controls**

### **1. Restricted Access IT Areas**

- a. Certain areas of Bellevue College will have restricted access. Some of these rooms are numbered, but are otherwise unidentified as to purpose and not specifically marked as secure areas. Personnel working in these areas will wear an approved college identification badge. These restricted access areas include:

<b>Network Server Rooms</b>	These rooms will be restricted by keypad and/or key access. Those having unescorted access will be limited to <u>authorized IR staff</u> and other Bellevue College staff specifically authorized by the Dean of Information Resources or designee. The doors are to remain closed and locked at all times.
<b>A110 Main Office</b>	The south (main) door to A110 will be unlocked from 8:00AM through 5:00 PM Monday through Friday (except holidays). The main office area will remain a public access area during these hours as long as IR employees are present. Access at other times will be restricted by keypad and/or key access. Exception: This office area may be locked during business hours if no personnel are working in the office (meetings, etc.). In this case, a notice will be posted identifying when the office will re-open.
<b>A110/A111 Work Areas</b>	These areas are non-public work areas. Those having unescorted access will be limited to authorized IR staff. All doors external to these work areas will remain closed and locked at all times and will be restricted by keypad and/or key access.
<b>N260 Work Areas</b>	The door to N260 will be open from 8:00AM through 5:00 PM Monday through Friday (except holidays), when IR staff are present. Only the internal entrance to the main office area will remain a public access area during these hours. Those having unescorted access to any other areas will be limited to authorized IR staff. Access at other times will be restricted by keypad and/or key access. <u>Exception:</u> This office area may be locked during business hours if no personnel are working in the office (meetings, etc.). In this case, a notice will be posted identifying how to contact Network Server Group personnel. All external doors to these work areas will remain closed and locked at all times and will be restricted by keypad and/or key access.
<b>Network and Phone closets</b>	The network and phone closets across campus will be restricted by traditional key access. When possible, lockable cabinets within these rooms will be used to provide an extra layer of security. Those having unescorted access will be limited to authorized IR staff. Outside vendors needing access to these areas will either be escorted by IR staff or check in with Campus Operations/ Public Safety to be temporarily issued a metal key, if authorized.
<b>Electrical closets</b>	Each electrical closet on campus, as well as the main power distribution closet, will be restricted by traditional key access. Those having unescorted access will be limited to authorized IR staff and the Facilities Engineer. Outside vendors needing access to these areas will either be escorted by IR or Facilities staff, or check in with Campus

	Operations/ Public Safety to be temporarily issued a metal key, if authorized.
<b>Phone Vault (A010)</b>	This facility will remain closed and locked at all times and will be restricted by traditional key access. When possible, lockable cabinets within this room will be used to provide an extra layer of security. Those having unescorted access will be limited to authorized IR staff that has been issued keys. Outside vendors needing access to these areas will either be escorted by authorized IR staff or check in with Campus Operations/ Public Safety to be temporarily issued a metal key, if authorized.
<b>North Campus Network Server Rooms</b>	These rooms will be restricted by key access. Those having unescorted access will be limited to authorized IR or Bellevue College staff specifically authorized by the Dean of Information Resources or designee. The doors are to remain closed and locked at all times.
<b>North Campus Building Entrance</b>	All card keys or keys that allow 7x24 main door access to North Campus will be authorized by the Continuing Education Site Manager.

## 2. Access Controls -- Keys and Key Cards

- a. Keys, proximity cards and/or access codes will be assigned to all authorized IR staff.
  - i Their access rights will be determined by their affiliation with IR and their specific job duties. This is roughly defined above.
  - ii Access codes will be treated like passwords and not shared with another person.
- b. Keys, proximity cards, and/or access codes will be assigned on an as-needed, permanent basis to Bellevue College employees only.
  - i Master keys will be issued on a restricted basis to authorized IR personnel, and to management and Campus Operations personnel.
  - ii All sub-master and individual office keys(e.g., for office doors, file cabinets, or desks), and proximity cards intended for permanent assignment to a Bellevue College employee on an as-needed, permanent basis, will be requested through Campus Operations using established procedures as described in the Bellevue College policy #6250: College Keys. At a minimum, this procedure will include:
    - A written request generated and approved by the administrator to whom the individual reports.
    - Approval of the appropriate Campus Operations authority.
    - A dated key card on file, signed by the individual, identifying the keys and/or proximity cards assigned.
  - iii Authorized employees needing temporary access to specific classrooms and labs will check-out keys or proximity cards on a one-day basis from Campus Operations or an authorized designee.
- c. Key assignments, access codes, and proximity cards will be reviewed no less than annually to assure that the assignments are still appropriate. Division/Department heads will review this report for their area and arrange for necessary key returns. Ideally, quarterly reviews should be done.
- d. If a key or proximity card is believed to be lost, it must be reported to the Campus Operations lock shop, the Public Safety office, and the employee's supervisor immediately.

- i In the event a metal key is lost or stolen, those doors that can be accessed by that key will be re-keyed at the discretion of the Campus Operations director. The related labor and material costs will be charged to the department or area budget, in accordance with Bellevue College policy #6250: College Keys.
- e. If an access code is believed to be compromised, it will be reported to the Campus Operations lock shop, the Public Safety office, and the employee's supervisor immediately, so that the code can be deactivated and a new code issued.
- f. Upon separation from college employment, any employee will surrender to Campus Operations all keys and proximity cards that have been assigned. The employee's supervisor will ensure that the Campus Operations lock shop has been notified so that person's access code can be deactivated.
- g. In addition to key-locked and access-coded doors, some Intermediate Distribution Facilities (Data closets, phone closets, switch closets; also known as "IDF") on campus have locked data cabinets. A secured lock box for spare data cabinet keys will be maintained in the IR server room. Campus Operations and/or Public Safety do not have keys to these data cabinets.
- h. Any students who have been authorized keys, but are not returning to the college for the next quarter, will turn in all keys and proximity cards before leaving the college.

### 3. Data Storage

- a. Until such time as it can be destroyed in compliance with the Bellevue College IT security standard addressing "Media Disposal", any waste or discarded output (including such things as paper, tape) containing sensitive data will be stored in a secure location.
  - i Sensitive documents (such as the college's check stock) will be stored only in designated secured cabinets.
  - ii Media (paper, tape, fiche) being prepared for distribution to SBCTC-IT will be maintained in the N260 area until it is picked up by Bellevue College Mail Services for SBCTC-IT delivery.
  - iii Portable storage media (such as tapes, CDs, diskettes) that have reached end of life (cannot be reused) will be magnetically or physically destroyed in compliance with the Bellevue College IT security standard addressing "Media Disposal."
  - iv Hard drives which have reached end of life (cannot be reused) will be magnetically erased and clean fill data will be recorded onto the entire drive or the drive will be physically destroyed in compliance with the Bellevue College IT security standard addressing "Media Disposal."
- b. Backup and system recovery media will be stored in physically secure locations at all times. These include all copies stored locally as well as those at an off-site storage facility. Access to backup media will be restricted to authorized IR staff and administrators.

### 4. Fire Suppression

- a. Fire suppression equipment will be provided for all computer rooms (including network and switch closets and server rooms). Fire suppression equipment will also be located in all telecommunications rooms.
  - i The fire suppression equipment will be a type designated for computer and electronic equipment.
  - ii Designated staff will receive periodic training on the use of the fire suppression equipment.

- iii The fire detection and suppression systems will be inspected and tested at least annually.

## **5. Flood/Water Protection**

- a. Extensive measures have been taken to prevent flooding in the main Phone Vault (A010), which includes: raising mission critical equipment on elevated flooring, resurfacing and sealing the entire floor, sump well/ submersible pump with a float switch pump, and water alarms monitored by Campus Operations. IR will ensure these systems are maintained and upgraded as necessary to keep the crucial campus systems housed in this IDF operational.
- b. Below ground electrical vaults will also be monitored and/or equipped with submersible pumps to prevent flooding, where deemed necessary by the IR Dean or authorized designee responsible for the facility.
- c. Designated staff will receive periodic training on responding to a flood situation. This training may be in the form of reviewing documentation instead of formal training.

## **6. Climate Control**

- a. All rooms containing computers will be provided with an adequate heating, ventilation, air conditioning (HVAC/DDC [Direct Digital Control]) system to assure computing equipment is maintained within its safe operating temperature.
  - i The preferred operating environment in labs, classrooms and offices is 68 - 77 degrees Fahrenheit at 40 - 60% humidity.
  - ii Network server rooms and switch rooms will be kept at a cooler temperature. The preferred operating environment in these rooms is 63 – 75 degrees Fahrenheit 40 - 60% humidity.
  - iii If the temperature in a room containing a computer exceeds 79 degrees, staff will continuously monitor the room's environment.
  - iv If the temperature in a room containing a computer exceeds 85 degrees, staff will notify Campus Operations and Dean of Information Resources or appropriate designee. If non-support staff, students, or faculty is present in a room at this temperature, the room will be evacuated until a return-to-normal temperature has been achieved.
  - v If the temperature in a room containing a computer continues to increase above 85 degrees, that room's doors will be opened and fans will be deployed. As all access controls will have been disabled to address an emergency temperature condition, staff will be responsible for closely monitoring access to the room.
  - vi If the temperature in a room containing a computer exceeds 95 degrees, all computing equipment will be shut down to prevent damage due to overheating. In addition to contacting Campus Operations and Dean of Information Resources or appropriate designee, representatives of the Network Server Group (NSG) and the Director of Computing Services will be contacted.
- b. Designated staff will receive periodic training on responding to HVAC/DDC failures. This training may be in the form of reviewing documentation instead of formal training.
- c. The climate control systems will be inspected and tested at least annually by a qualified technician.

## **7. Electrical Power and Backup Power**

- a. All network server systems will be provided backup power via an uninterruptible power system (UPS) and/or a standby generator. Enough UPS' will be used to provide backup power for all servers in the rooms.

- b. Additionally, the Campus PBX system and Qwest T1 equipment will have multiple UPS' installed to support their uninterrupted operation.
- c. Designated IR support staff will receive periodic training on responding to power failures. This training may be in the form of reviewing documentation instead of formal training.
- d. The UPS and backup power generation systems will be inspected and tested at least annually by a qualified technician.

## 8. Evacuation Planning and Building Safety

- a. Emergency information, including building evacuation plans will be posted in all computer classrooms, labs, offices, work areas, and server rooms in compliance with Bellevue College Public Safety policies and procedures.
- b. Emergency telephones in Bellevue College elevators ring directly to Bellevue College Public Safety and will be used in the event of an elevator failure.
- c. All designated work areas will be equipped with an emergency first aid kit, and all staff members will be trained in its use. This training may be in the form of reviewing documentation instead of formal training.
- d. The evacuation plan will be tested at least annually.

## 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. SBCTC-IT Security Standard—*Physical Security*
2. Bellevue College Policy #5250: *Information Technology (IT) Security*
3. Bellevue College Policy# 5300: *Computer Labs*
4. Bellevue College IT Security Standard: *Employee Security Training*
5. Bellevue College IT Security Standard: *Media Disposal*
6. Bellevue College policy #6250: *College Keys*

Effective Date:  
Date Last Modified:

July 2003  
April 12, 2009