



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

IT Security Standard:

Connecting Non-Bellevue College Equipment to the Bellevue College Network

Introduction

This standard defines the steps implementing the Bellevue College IT Security Policy for non-Bellevue College managed equipment connecting to the Bellevue College internal network. The purpose of this standard is to assure the integrity and reliability of the Bellevue College networks and all components of those networks. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines the expectations and requirements for campus technology users attaching non-Bellevue College equipment to the Bellevue College network. The primary focus of this standard is workstation class equipment, devices attached to them and non-computer devices using the network directly.

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 networked components protected through implementation of this standard are critical infrastructure to the daily business and instructional operations of Bellevue College. These components include everything from switches and routers, to computer workstations and servers. Some of the college's business (administrative, instructional, and public service) functions can be significantly interrupted because of a network disruption caused by attaching foreign devices to the network.

Given the high level of dependence on the networked services, the most significant threats are:

1. Accidental and/or malicious rapid spread of malicious code within the network perimeter.
2. Accidental and/or malicious denial of service.
3. Malicious and/or unauthorized access to resources or data.

In assessing the nature of the asset and the nature of the threat, the primary risk associated with unauthorized components being attached to the network is interference with expected services. This loss of service does have associated risks of loss of revenue, dissatisfaction of those to whom Bellevue College provides services, interruption of productive work, and to some degree a loss of reputation.

Secondary to these threats is the potential for inappropriate use of the resource. This can include such things as excessive bandwidth use, theft or modification of data, uses inconsistent with Bellevue College's mission, or uses that are in violation of state and federal law and/or Bellevue College acceptable use policies.

Standard

A. Introduction

1. A variety of technology hardware (hereinafter collectively referred to as "equipment") can communicate through wired or wireless connections with modern telecommunications networks. This equipment can be different types of computer workstations and laptops, portable devices such as personal digital assistants (PDA), hand-held scanners, printers, digital cameras, digital music appliances (such as an MP3 player), digital projectors and other telecommunications devices such as telephones.
2. While many types of this equipment are attached and used daily on Bellevue College's networks, protection of that resource requires careful management of all such components on the network. Bellevue College IT support staff install and maintain all Bellevue College owned equipment of this type.
3. Before making a wired connection of any non-Bellevue College owned equipment directly to the Bellevue College network, or to another device connected to the network, a campus user must certify to Bellevue College technical support staff that all conditions identified in this standard have been met.
 - a. Non-Bellevue College owned equipment may be connected wirelessly to the Bellevue College network following the procedures and standards identified in the Bellevue College IT security standard addressing "Wireless Network Configuration."
4. "Non-Bellevue College owned equipment", in the context of this standard, is defined as computing, networking, video, and telecommunications equipment not owned by Bellevue College and/or not maintained or managed by authorized Bellevue College technical support personnel or authorized designees.
 - a. **Note:** If the equipment is a portable data storage device, its use is governed instead by the "Non-Bellevue College Owned Devices" section of the Bellevue College IT security standard addressing "Portable Data Storage Devices."
5. When non-Bellevue College owned equipment is to be connected to the Bellevue College network, a formal request will be made to Information Resources and approved by an authorized IR administrator.
 - a. If the requestor is not a Bellevue College employee, all applicable expectations of the Bellevue College IT security standard addressing "Non-Employee Access to Bellevue College Systems" must be complied with before non-Bellevue College equipment may be connected to the Bellevue College network.
 - b. The requestor must sign the form at Appendix B (Non-Bellevue College Equipment Form), below, indicating agreement to abide by this standard. This form must be delivered or mailed to the Bellevue College Help Desk and approved by an authorized IR Administrator (or authorized designee) prior to connecting any equipment to the Bellevue College network. Upon approval, the form will be kept on file by the Bellevue College IT Security Administrator and/or approving administrator.
 - c. The equipment owner must review and abide by all applicable copyright and licensing policies. These include, but may not be limited to: Bellevue College's IT Security and

Software Licensing Compliance policies and state and/or federal law. The equipment owner must also review and abide by all applicable Bellevue College acceptable use policies.

- d. The equipment will not be incorporated into the Bellevue College Microsoft Windows domain structure or automatically granted access to other internal services (e.g., email accounts). Requests for additional access to network resources will be handled on a case-by-case basis and processed through adherence with applicable Bellevue College policies and procedures. Any Bellevue College Web-based services will be available to the user through the Internet, if the equipment has Internet capabilities.
- e. In support of non-Bellevue College owned computer equipment being used on campus, Bellevue College technical support personnel can, by law, provide information and advice only. Bellevue College technical support personnel will not support or configure non-Bellevue College equipment.
- f. Antivirus protection is the responsibility of the workstation or device owner. High-quality, current antivirus software must be installed and running on the non-Bellevue College equipment, if applicable. Weekly, or more frequent, disk virus scans will be performed by workstation owners on each non-Bellevue College workstation. Antivirus pattern files will be kept current.
- g. Any software requiring installation on a Bellevue College owned workstation to facilitate use of attached non-Bellevue College owned equipment will be considered “personally-owned” and will be handled using the procedures and standards identified in the “Use of Personal Software for Work Purposes” section of the Bellevue College IT security standard addressing “Software Management.”
- h. Maintenance of the equipment and the equipment’s operating system and applications, if used by the equipment, is the responsibility of the workstation owner.
 - i) This maintenance includes, but is not limited to file system backups, equipment administration and security.
 - ii) The owner must apply current security-related patches for all operating systems and installed applications prior to connecting the equipment and make any subsequent upgrades and applications in an expedient fashion.

B. Non-employee Equipment Requirements and Process

1. At times, non-employees such as vendors or guest lecturers need to connect non-Bellevue College owned equipment to the Bellevue College network or to another device connected to the Bellevue College network. Such connections will be granted only for short-term use (up to a few hours), for the duration of the specific event requiring such access. Once the purpose for which the equipment was connected to the network has been completed, the device will be removed.
2. All connectivity needed by visitors who are not Bellevue College employees will be coordinated through a Bellevue College contact person. Permission to connect non-employee equipment will be granted only after the following has been provided:
 - a. The Bellevue College employee acting as contact person for the non-employee user will be responsible for submitting an appropriate request for this type of connectivity to Request Center, and for communicating any necessary information to the visitor.
 - b. Non-employee users will sign the “Non-Bellevue College Equipment Form” (Appendix B, below) indicating they agree to abide by this standard and other applicable Bellevue College policies and standards. This form will then be delivered or faxed to the Help Desk at least 1 week in advance of the expected need.
 - c. The Help Desk must be notified of the specific location the non-Bellevue College equipment will be connected, including room number and specific network port within the room.

- d. If applicable, non-employee users will be required to provide the Help Desk with the specific hardware address for the network card on their equipment (Media Access Control or “MAC” addresses) so that connectivity with the appropriate network can be established. This requirement is dependant on the type of equipment being used.
3. The request will be routed through the Bellevue College IT Security Administrator, or an authorized designee, to the appropriate IR support unit for technical review and processing.
 - a. Any technical or network problem with the request will be discussed with the requesting individual for correction or reconfiguration.
 - b. Once all issues are resolved, an authorized IR administrator will review the appropriateness of the request, and grant or deny approval.
 - c. Both the requesting individual and Bellevue College contact person will be notified of the disposition of the request.

C. Employee-owned Equipment Requirements and Process

1. Bellevue College employees may make repeated connections of their non-Bellevue College owned equipment at different locations on campus on a regular basis. All connections to the Bellevue College network using equipment that is personally-owned by Bellevue College employees will follow this process for each piece of equipment and for each location where a connection to the Bellevue College network is made:
 - a. The Bellevue College employee will submit an appropriate request for connectivity to Request Center.
 - b. Employee users will sign the “Non-Bellevue College Equipment Form” (Appendix B, below) indicating they agree to abide by this standard and other applicable Bellevue College policies and standards. This form must then be delivered or mailed to the Bellevue College Help Desk.
 - c. If applicable, employee users will be required to provide the Help Desk with the specific hardware addresses for the network cards on their equipment (Media Access Control or “MAC” addresses) so that appropriate connectivity can be established.
 - d. Employee users will notify the Help Desk of the specific location(s) where the non-Bellevue College equipment will be connected, including room number and specific network port within the desired room. If the user expects to use the equipment in multiple locations, each location must be identified so that the appropriate network configuration may be made. One copy of the signed form is sufficient for all requested campus locations for a specific single device.
 - e. The request will be routed through the Bellevue College IT Security Administrator, or an authorized designee, to the appropriate IR support unit for technical review and processing.
 - i) Any technical or network problem with the request will be discussed with the requesting individual for correction or reconfiguration.
 - ii) Once all issues are resolved, an authorized IR administrator will review the appropriateness of the request, and grant or deny approval.
 - iii) Long-term connections of any non-Bellevue College equipment will be reviewed annually.

D. Non-Bellevue College owned Servers, Networking, and Telecommunications Requirements

1. Non-Bellevue College owned equipment of this class is not allowed on the Bellevue College network if Bellevue College technical support staff or an authorized designee does not install and manage it. Exceptions will be handled on a case-by-case basis, and all due care will be practiced to assure such exceptional equipment does not jeopardize the security, integrity, or reliability of

data or services on the Bellevue College network. All exceptions will be approved by the IT Security Administrator or an authorized IR administrator.

E. Information Resources Response to Problems

1. If non-Bellevue College equipment is determined to be compromised in any way or identified as the cause of problems on any Bellevue College network, Bellevue College technical support staff will define the appropriate remedies.
 - a. This will include disconnection of the questionable equipment from any Bellevue College resources immediately and without warning. Best efforts will be made to notify the equipment owner of the problem and this solution prior to disconnection.
 - b. Remedies will include a request for a specific cleanup procedure, up to and including a request for the equipment owner to reinstall any applicable software or operating system.
 - c. If identified issues are not addressed by the equipment owner in a timely fashion, network connectivity will be discontinued until the questionable equipment is physically removed from the network.

F. Authority

1. The Dean of Information Resources will be responsible for designating those IR administrators or authorized designees authorized to approve or deny requests made under the provisions of this standard.

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

1. CIS IT Security Policy, January 29, 2003
2. CIS IT Security Standard: Connecting Non-CIS Computer/Telecommunications Equipment to CIS Networks, January 29, 2003
3. Bellevue College Policy #5250: Information Technology (IT) Security
4. Bellevue College Policy #5150: Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems
5. Bellevue College Policy #5000: Acceptable Use of Bellevue College Computers
6. Bellevue College Policy #4400: Acceptable Use of State Resources
7. Bellevue College IT Security Standard: Software Management
8. Bellevue College IT Security Standard: Portable Data Storage Devices
9. Bellevue College IT Security Standard: Data and Information Security

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