



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

IT Security Standard:

Wireless Network Configuration and Management

Introduction

This standard defines the steps necessary to implement the Bellevue College IT Security Policy within the context of configuring of campus wireless networks. The necessity for this standard is to assure the integrity and reliability of the Bellevue College internal networks, the computers on those networks, and the software installed on those computers. The standard will be reviewed annually or when changes are implemented.

Scope

This standard defines the processes and controls related to using wireless connections to the Bellevue College computing networks. It applies to all such connections, whether they are made to the Administrative or the Academic Networks. It is expected any deviations from this standard for either business necessity or platform implementation constraints will be appropriately documented with the Bellevue College IT Security Administrator.

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 use of wireless connections to access the Bellevue College networks removes a significant security control traditionally in place to protect those networks. Access has previously been limited to wired connections from locations on campus and the configuration of computers to connect to the network has been controlled by support personnel. The use of wireless connections will make potential access to the networks much more ubiquitous and will, in effect, eliminate most physical controls that are in place which limit access.

Additionally, the campus users utilizing wireless access generally will not have sufficient grasp of the basic security issues related to network use and integrity. Thus, a clear standard delineating the use of wireless connections becomes a critical factor in assuring the security of the computing and communications resources under Bellevue College's responsibility.

Given the high level of dependence on the Bellevue College networks to accomplish the educational and business missions of the college, the most significant threats are:

1. Malicious and/or accidental use of wireless access to perform actions designed to usurp Bellevue College systems and their operation
2. Malicious and/or unauthorized access to controlling components (e.g., routers, DNS, domain controllers)
3. Malicious and/or unauthorized access to data and or processes
4. Theft and/or malicious changing of data
5. Accidental and/or malicious destruction or disclosure of critical data

Because of the nature of the asset and the nature of the threat, all risks associated with the use of wireless network access on campus are very significant. Any misuse or loss of the networking resources could put the college instructional and business systems at great risk, with potential significant loss to Bellevue College.

Standard

General

All access to Bellevue College networks through wireless means will require the same compliance for password-controlled access and for appropriate use as does any wired connection.

1. Only employees, students, and non-employees authorized in accordance with the Bellevue College Acceptable Use of the Bellevue College Network and the Bellevue College Data Management Systems Policy will be able to obtain wireless access.
2. All wireless access on campus to the Bellevue College networks will be configured to meet the same standards for authentication and authorization as required for wired connections.
3. All wireless users will meet the expectations for appropriate use as described in the Bellevue College Acceptable Use of State Resources Policy, the Bellevue College Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems Policy, and the Bellevue College Acceptable Use of Bellevue College Computers Policy (if applicable).
4. Because wireless transmissions are significantly easier for outside entities to monitor or intercept, the wireless network will never be used as the means for transmitting any confidential information.
5. Bellevue College does not have wireless access point connections from the Bellevue College network that are connected to or part of the State Governmental Network (SGN). If Bellevue College does determine that it would be feasible and cost-effective to implement web-based applications within the SGN, all rules, standards and guidelines as prescribed by DIS/ISB will be followed and the DIS Senior Technology Management Consultant will be contacted.

Servers and Databases

Servers supporting wireless transmissions on campus are configured the same as wired servers. However, the practice of verifying access through hardware MAC addresses requires configuration of a database to store the information with a means to query that data. The specifics of that setup will be at the discretion of the IT Systems Administrator responsible for the wireless network and will follow these guidelines:

1. The path and escalation of privileges will follow this general path:
 - a. User connects to the Access Point.
 - b. The firewall provides for and protects the first level of network access.
 - c. The Radius server acts as the interface between the Access Points and the SQL Server for authentication.
 - d. The SQL Server maintains the MAC address database and usage logs.
 - e. VPN provides the enhanced network access.
2. All wireless access points will meet the standards defined in the Bellevue College IT Security Standard addressing "Network Device Configuration."

3. All databases used to support wireless access will meet the standards described in the Bellevue College IT Security Standard addressing "Database Management."

Bellevue College-owned Workstations

Most Bellevue College-owned workstations using the wireless network will be laptops. Users needing to have their computers configured to access the network(s) via wireless will make a request through the Help Desk. The user will be required to bring the computer into the Help Desk to accomplish this.

1. In order to gain first level, Web-only (HTTP Port 80) access to the Internet through the wireless network:
 - a. The computer's MAC address will be registered with Information Resources. The attending technician will be responsible for obtaining this information.
 - b. The device will be configured for use of the campus Access Points as network connections.
 - c. The computer will be configured to verify with the Radius server that the MAC address is valid when the user connects through an Access Point. If valid, the computer will be granted first level access. If not, access will be denied.
2. Once first level access has been granted, an individual can then use the current Virtual Private Network (VPN) client to gain more access to the specific internal Bellevue College network(s) for which they have authorization.
 - a. To utilize the VPN, the client software will be installed on the system and configured with the correct VPN profile. This will enable the user to click on an icon on the desktop of the computer to connect through the VPN with 168 bit encryption and increased access to resources.

Non Bellevue College-owned Workstation

Bellevue College technical support personnel will not configure personally-owned computers or handheld devices. Authorized users wanting to configure their personally-owned computers or handheld devices to access the Internet through Bellevue College's wireless connection have a Web site available to assist them in registering their MAC address and system type to a wireless configuration. Users must have an active login account on the Bellevue College Administrative or Academic Networks to be able to register their personally-owned computers or handheld devices for wireless access.

1. Access through the wireless network by computers or devices of this type will be Web-only (HTTP Port 80) access to the Internet.
2. Bellevue College's wireless connections are shared. Any overuse by one user which affects access for others will result in the user losing his Internet connection.
3. **Student Access**
 - a. Student access to the wireless network will only be active for the quarter in which the student is currently enrolled.
 - b. At the end of each quarter, all student access will be removed.
 - c. Students enrolled for the subsequent quarter will be required to re-register their equipment through the Web site after the quarter begins.
4. **VPN**
 - a. The Web site providing self-registration for the purposes of wireless access will have an option available to the user to download the Cisco VPN client.
 - b. This client software will be installed on the system and configured with the correct VPN profile for the user to gain authorized access to specific internal Bellevue College network(s).
 - c. Instructions regarding how to do this will be available on the Web site.

Monitoring and Administration

1. IR personnel authorized by the Dean of Information Resources or an authorized designee will actively monitor all wireless connections to the Bellevue College Network to ensure compliance

with this standard, with the Bellevue College IT Security Standard addressing “Intrusion Detection and Incident Response” and with all Bellevue College acceptable use policies.

2. All wireless access activity to Bellevue College networks will be logged in the SQL database.

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. Bellevue College Acceptable Use of State Resources Policy
2. Bellevue College Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems Policy
3. Bellevue College Acceptable Use of Bellevue College Computers Policy
4. Bellevue College Software Licensing Compliance Policy
5. Bellevue College IT Security Standard: Password Management
6. Bellevue College IT Security Standard: Intrusion Detection and Incident Response
7. Bellevue College IT Security Standard: Network Device Configuration
8. Bellevue College IT Security Standard: Database Management

Effective Date: July 2003
Date Last Modified: July 10, 2009