

IT Security Standard:

Internet Software Security

Introduction

This standard defines the steps needed to implement Bellevue College policy # 5250: Information Technology (IT) Security with regard to securing the use of software applications which access the resources available through the Internet. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines specific requirements for the secure use of the resources available through the Internet and software used to access the Internet from Bellevue College.

This standard is not intended to supersede the Bellevue College IT Security Standards addressing "Applications Development", "Web Servers", or "Web Space Usage", but rather to compliment them with respect to broader, Internet-wide issues raised by the Washington state Information Services Board (ISB).

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 Internet provides access to a number of services, including e-mail, file transfer, access to remote systems, interactive conferences, news groups, the World Wide Web, and others. The software allowing access to the Internet, including web browsers, e-mail clients, file transfer tools and other desktop applications may introduce vulnerabilities to the Bellevue College networks. As these resources are infrastructure critical to the daily business and operations of the college, Bellevue College's business functions would be severely impacted with significant disruption in Internet access and/or access to the services available.

Given the increasing level of dependence on Internet-based services, the most significant threats are:

1. Malicious and/or unauthorized modification to Bellevue College systems and networks.
2. Malicious and/or unauthorized disclosure and/or modification of data.
3. Compromise of Web servers or other Internet activated infrastructure.
4. Denial of service.

Given the nature of the asset and the nature of the threat, the main risks associated with use of the Internet are these malicious attacks. All of these threats 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.

Standard

A. General

1. All software used to access the Internet from the Bellevue College networks must be approved by the Dean of Information Resources or authorized designee before installation. Only approved versions of software may be used. IR will maintain a list of such approved applications.
2. Installation of software used to access the Internet will only be performed by authorized IR support personnel, in compliance with the Bellevue College IT Security Standard addressing "Software Management", and must incorporate all current and updated security patches appropriate to the Bellevue College networking and internetworking environment.
3. Internet software installations will be configured by IR support personnel to use appropriate technology to prevent the disclosure of, or to obscure, IP addresses beyond the Bellevue College network, if possible.
4. All access to Internet resources from Bellevue College will be provided only through appropriate channels, as approved by the Bellevue College IT Security Administrator and/or the Dean of Information Resources (IR), or authorized designee.
5. This access will be set up and maintained by Information Resources support personnel, or authorized designees only.
6. Appropriate anti-virus software (as defined by the Bellevue College IT security standards addressing "Virus Protection") will be installed on all workstations and configured to ensure that files received from the Internet are checked for viruses.
7. Units and individuals are prohibited from establishing permanent or sustained Internet connections via an Internet Service Provider (ISP) from any Bellevue College-networked workstation which bypasses the Bellevue College firewall. This prohibition will be strictly enforced, as it provides an unmonitored entry path from the Internet into the Bellevue College network, which can lead to unintended security risks
8. Transmitting non-encrypted confidential information, as defined by Bellevue College policy #1500, "Access to Public Records" and by the federal Family Education Rights and Privacy Act (FERPA) is strictly prohibited.
9. All software providing access to any Internet resources will be updated and maintained regularly in accordance with the Bellevue College IT security standard addressing "Patch Management."

B. Web Servers

1. Web servers can be attacked directly or used as jumping-off points to attack Bellevue College's internal networks. Therefore, in addition to the standards and authorized configurations articulated in the Bellevue College IT security standard addressing "Web Servers", the following standards apply to web server software:
 - a. Campus users are forbidden from downloading, installing, or running any Web server software without prior approval from the Bellevue College IT Security Administrator and/or the Dean of Information Resources (IR), or authorized designee, and their unit administrator.
 - b. All remote control of Web servers, including administrator operations and/or supervisor-level logons, will be done using properly secured sessions utilizing passwords in compliance with the Bellevue College IT security standard addressing "Password Management", which provide prerequisite high confidence level authentication.
 - c. Any installed Web server software and the software of the underlying operating system will employ all security patches and configuration options appropriate to their use at Bellevue College.

- d. Web servers that are accessible to the public will not serve as a repository for confidential data. However, a public Web server can act as a proxy for access to confidential data located on secure servers.

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 #5250: “*Information Technology (IT) Security*”
2. Bellevue College Policy #1500: “*Access to Public Records*”
3. Bellevue College IT Security Standard: *Applications Development*
4. Bellevue College IT Security Standard: *Web Servers*
5. Bellevue College IT Security Standard: *Web Space Usage*
6. Bellevue College IT Security Standard: *Password Management*
7. Bellevue College IT Security Standard: *Virus Protection*
8. Public Law 93-380, the Family Educational Rights and Privacy Act of 1974 (FERPA)
9. DIS, *Information Technology Security Standards*,
<http://isb.wa.gov/policies/portfolio/401S.doc> , 2006

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