



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

IT Security Standard:

Web Servers

Introduction

This standard defines the steps needed to implement the Bellevue College IT Security Policy for Web servers and applications. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines specific procedural and configuration elements for management of Web servers in support of the Bellevue College IT Security Policy. This includes all platforms that Web servers are implemented onto, namely Microsoft Windows with IIS and Unix with Apache. In general, this standard will apply to Web servers used in development and production. It is recognized that the development environment will be more loosely defined, and this document tries to clearly differentiate where those two environments diverge from a common definition.

This standard only applies to network connected devices; standalone, non-networked devices (such as might be used for some otherwise non-compliant development effort) are outside the scope of this standard.

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

Web servers and the application software that runs on them are fast becoming critical infrastructure to the daily business and operations of Bellevue College. Business functions at Bellevue College would be severely impacted with significant network or web server disruption.

Given the increasing level of dependence on web-based service, the most significant threats are:

1. Malicious and/or unauthorized modification to web content
2. Malicious and/or unauthorized disclosure, modification or loss of application data
3. Compromise of Web server
4. Denial of service
5. Malicious and/or accidental physical damage or theft of Web server computer systems

Given the nature of the asset and the nature of the threat, the main risks associated with Web services are 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. In the event of damaged or stolen equipment, another associated risk may also be the replacement cost of that equipment.

Standard

Operating System

1. The hardware and software operating environment of a Web server will be maintained in compliance with the applicable Bellevue College IT security standards addressing physical and operating system security.
2. With the occasional exception of experimental Web server installations that are not connected to the network, Web servers will not be configured or allowed on non-server workstations.

Web Server

There is a tremendous amount of commonality across Web servers (e.g., Microsoft IIS and Apache), but there are also some distinct differences. This standard attempts to address Web servers as a single class of applications, focusing on their commonality. Where there are specific platform differences, an attempt has been made to identify those.

When creating a Web server, the Network Server Group (NSG) systems administrator will follow the security best practices for configuration and management as defined by the vendor or user community for the given Web server software. Additionally, the following criteria will be followed:

1. If possible, Web servers will be located on computers dedicated solely to that purpose.
2. The Web server will be installed with the minimal necessary installation and configuration.
3. All application patches will be current.
4. The Web content will be installed on a separate disk partition from the operating system and applications.
5. The Web server will execute as a non-privileged user of the operating system.
6. Within the Microsoft IIS configuration, the Application Protection option will **not** be set to "Low (IIS Process)", as these processes run with Local System privileges.
7. All sample and test components will be removed.
8. All vendor provided installation, test, and sample configuration documentation will be removed. This is not intended to include end user help pages and end user documentation. Development servers and intranet servers inside the firewall are excluded from this requirement.
9. Any program interpreters from the Web server's document root and CGI scripts directories will be removed.
10. The default display of directory (folder) contents will be removed. This is sometimes referred to as directory indexing or directory browsing on Web servers that are exposed to the Internet.
11. All Web server (HTTP) headers that provide information on platform, add-in software products, modules, and version will be disabled or minimized.
12. The Web server, and all application processes spawned from the Web server, will be allowed to read, but not to write to files and directories where Web content is stored.
 - a. The Web server will write to log files but will not be granted read access to them.
 - b. Any temporary files created by the Web server (or its spawned application processes) during processing will be maintained in a protected sub-directory, and access to those files will be restricted to the Web server process.
 - c. All CGI programs (spawned executables) for the Web server will be maintained in a small number of directories (preferably one) under the exclusive control of the Web server

administrator (most likely the systems administrator). The Web administrator will be the only one allowed to maintain those directories.

Server-side scripting tools (e.g., Microsoft's ASP, GNU PHP, Macromedia Cold Fusion) are not included within this requirement.

13. There are numerous ways, by design, to traverse the file system to locations outside the document root. These include: symbolic links, virtual directories/paths, as well as using the "file://" protocol to an available Window's share. These can break the security controls implemented on the Web server and will be disabled, deleted, or otherwise not used.

User Access Controls and Confidentiality

1. IP Address restriction will be used, where there are clearly delineated audiences, to control who may access a particular Web site. This is not a strong security device; if the function or content of the site is sensitive, address restrictions must be used only as a secondary security device.
2. For applications that process user/customer or other sensitive data, data confidentiality protection will include:
 - a. SSL with 128 bit keys will be used
 - b. Weak ciphers and short key lengths will be explicitly disallowed to prevent "falling back" to an insecure operation mode. DES and 3DES will be avoided for both security and performance reasons. AES with a 128 bit key or greater is preferred, although other strong ciphers may also be used.

If strong authentication is required, the site will use authentication layered on top of SSL encryption.

Web Server Logging

1. Error and access logs of production Web servers will be reviewed daily to identify problems and attempted server abuse (attacks). Members of the NSG will conduct this review. Ideally, this will incorporate some level of automation for at least first-pass filtering.
2. For addressing security considerations, the following fields, or their equivalents, will be configured for logging: system date and time, time zone, client IP address, port used to access the server (destination port), user name (for authenticated connections), method (e.g., GET, POST), the full URL requested (server name and file path), the status of the request, and the number of bytes transferred. Other information may, and should, be included if indicated by other organization standards, or industry best practices.
3. Web logs may contain sensitive information that is protected by the Public Records Privacy Protection Policy or other statutes. Care will be taken to prevent accidental disclosure of this information.

Web Content

Web content, for this section, will refer only to that content that the Bellevue College publishes as documentation and information to its users, its business partners, and the public. This content is often "static" pages, and retrieval of documentation that has been archived in a Web-accessible repository.

Public Web servers will not be used to host sensitive information intended to be accessed only by internal users. In other words, an Intranet and an Internet Web server may not be run on the same computer.

1. Public Web servers must prominently display a link to the site's privacy policy. This was mandated by the ISB on 12 June 2001 (Public Records Privacy Protection Policy, see references below).
2. Providing and managing the actual Web content is a cooperative and collaborative effort that includes staff from every Bellevue College unit, all of whom are expected to be aware of and sensitive to the following issues with regards to the information published on the Bellevue College Web sites. Bellevue College's Webmaster will have ultimate responsibility for managing content on all Bellevue College Web sites. This will include such tasks as:
 - a. Identifying what content should be published to a Web site.
 - b. Reviewing the content for possible negative ramifications for publishing.
 - c. Identifying who should be responsible for creating and maintaining the content.

- d. Reviewing the information for sensitivity and distribution control.
- e. Determining the appropriate access and security controls.
- f. Periodically reviewing the Web site for sensitive information that may be stored (hidden) in the server side scripting source code (e.g., ASP, PHP) or form.

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 IT Security Policy
2. CIS Standard on Web Servers
3. Tracy, Jansen, McLamon, *Guidelines on Securing Public Web Servers*, NIST, Feb. 2002.
4. Fosenen, *Securing Internet Information Server 5.0*, SANS, May 2001
5. Rhoades, *Auditing Web-Based Applications*, SANS, 2002
6. Peteanu, *Best Practices for Secure Web Development*, http://www.blazonry.com/devnotes/secure_webdev-3.0.pdf, 2000
7. Curphus, Endler, Taylor, et al, *A guide to building Secure Web Applications*, <http://www.owasp.org/guide/>, The Open Web Application Security Project, 2002,
8. DIS, *Public Records Privacy Protection Policy*, <http://www.wa.gov/dis/portfolio/publicrecordsprivacyprotectionpolicy.htm>, 2002
9. CIS, *Model College Privacy Notice*, <http://www.cis.ctc.edu/wctc/policies/CollegePrivacyNotice.htm>, 2002

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