



IT Security Standard:

Windows Server Configuration

Introduction

This standard defines the steps needed to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding Windows-based servers deployed on campus. This 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 Microsoft Windows-based operating systems in support of the Bellevue College IT Security Policy. It addresses configurations which apply to server installations only. General workstation configuration is addressed in the Bellevue College IT Security Standard entitled "Windows Base System Configuration." The general standard applies to both administrative and student systems; all specific exceptions for student computers will be identified in the exceptions document.

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 computing resources within the scope of this standard are critical infrastructure to the daily business and operations of Bellevue College.

Given the high level of dependence on these server systems, the most significant threats are:

1. Malicious denial of service
2. Maliciously installed viruses, Trojans, and worms (malicious Code)
3. Malicious and/or unauthorized access, elevating user privilege or system privilege levels
4. Interruption to electrical power or other environmental problems
5. Accidental and/or malicious physical damage
6. Theft of computer resources
7. Malicious and/or unauthorized access to sensitive data for theft or fraud

Given the nature of the asset and the nature of the threat, the primary risk associated with Windows servers is loss of service. This loss of service does have associated risks including: 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, there is also a risk involving the replacement cost of that equipment.

Secondary to these threats is the potential for inappropriate use of the resources. This threat is greater for any servers that may be on the Student Network. This can include such things as: excessive bandwidth use; uses inconsistent with Bellevue College's organizational mission; and uses that are in violation of the applicable Bellevue College Acceptable Use Policies, or federal and/or state law.

Standard

A. Introduction

1. The Bellevue College IT Security Standard addressing "Windows Base System Configuration" applies to the setup and use of Windows server configurations. All of its expectations not specifically identified in this document will be followed.

B. Initial Build

1. In addition to meeting the "Initial Build" requirements listed in the Bellevue College IT Security Standard addressing "Windows Base System Configuration," systems configured as servers will also comply with the following:
 - a. Subsystems unnecessary to the business application of the server (such as OS/2 and POSIX) will not be installed.
 - b. Simple Network Management Protocol (SNMP) will not be enabled on server-class computers.
 - c. Modems will not be configured for servers.
 - d. The system will be configured so that it will not reboot without user intervention.

C. Physical Security

1. Physical security for Bellevue College server systems will be in accordance with specifications of the Bellevue College IT Security Standard addressing "Physical Security."

D. Services

1. Most of the common "business" services (such as DNS, Web, Email, and Databases) will have Bellevue College security standards defined specifically for them. All services not necessary to support the business or educational use of the computer will be disabled. However, all services needed to accomplish the business or educational purpose of the system will be available for use.

E. Backups and System Recovery

1. System recovery media (tape, CD, floppy...) will be created and kept current so the system can be recovered to a known good state in the event of a system failure or compromise.
2. System recovery documentation, outlining how to recover a system from scratch, will be available on paper or digital media.
3. The recovery media and documentation will be stored in a location providing restricted access control, known to all systems administration staff and the IR IT Management Team. These locations will be reasonably accessible.
4. Backup cycles will vary by system, subject to the nature of the server's task and the data stored on the server. The IT systems administrators for each system will determine the most appropriate backup scenarios for the servers for which they are responsible.
5. Backup media will be kept in a four-week rotation with one week being kept at an offsite data storage facility.

F. Account Management

1. All expectations of the Bellevue College IT Security Standard addressing "Password Management" will be followed. In addition, server configurations will meet the following:
 - a. The Guest account will be set to disabled.

- b. All users will have their own account to log into. Account sharing (except for IT systems administration accounts and those noted in the *Password Management Exceptions* document) will not be permitted.
- c. Accounts are granted for specific business need, the account will be expired (deactivated or deleted) when that need no longer exists.

G. Elevated Privileges

1. Systems Administrators will maintain two accounts: one with standard user privileges and a second with administrator privileges. They will use the standard account for their day-to-day work and execute programs requiring privilege with the "run-as" option. In those cases where extended work at the elevated privileges level cannot be avoided, then an authorized IT network administrator will directly log into the assigned administrative account.
2. IT System Administration privileges (and responsibilities) will be granted only to authorized IR IT support personnel. On occasion, other trained staff in IR units will be granted such privileges as necessary to perform their duties.
3. Upon an individual's separation from Information Resources, all privileged access to the Windows servers will be revoked. Upon separation from Bellevue College, all access to Bellevue College systems will be revoked.

H. System Monitoring

1. A file system integrity checker will be run on a regular basis and reviewed for discrepancies the following morning. The frequency of the run will be determined by the exposure of the server to high risk environments. Servers exposed to the Internet will be scanned daily. Servers in more secure environments will be scanned no less than weekly.
2. Basic "health" monitoring will be performed on each server. The IT network administration staff will monitor the general health report screen fairly continuously.
3. Web-based system management tools will be used if they comply with the following:
 - a. The tool has secure user level authentication
 - b. The tool can only be used on/within a secure network, not across the State Board for Technical and Community Colleges – Information Technology (SBCTC-IT) or K20 network.
 - c. The use of Secure Socket Layers (SSL) is highly recommended.
4. Configuration tools which are restricted to only allow connections from their loopback address will be allowed.

I. Logging and Log Review

1. Logging may be done to a central log host for consolidated storage and processing. However, if this is done, local logs will be kept as well. This will include all system and application (web, email...) logs.
2. Logs will be maintained for no less than a week on the system and an additional four weeks on backup media.
3. The logs will be reviewed no less than daily for security and O/S or application issues which need attention.

J. System Scan/Assessment

1. Systems will receive periodic (no less than once a quarter) network vulnerability scans. Within the limitations of business need, all vulnerabilities identified will be quickly rectified. It is recommended that different tools be used periodically as each has different strengths.
2. Assessment reports will be forwarded to the Bellevue College IT Security Administrator and/or Dean of Information Resources to be reviewed and filed.

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 #4400, *Acceptable Use of State Resources*
2. Bellevue College Policy #5000, *Acceptable Use of Bellevue College Computers*
3. Bellevue College Policy #5150, *Acceptable Use of Bellevue College Networks and Systems*
4. Bellevue College Policy #5250 – *Information Technology (IT) Security*
5. Bellevue College IT Security Standard: *Security Privileges*
6. Bellevue College IT Security Standard: *Password Management*
7. Bellevue College IT Security Standard: *Software Management*
8. Bellevue College IT Security Standard: *Windows Base System Configuration*
9. SBCTC-IT IT Security Standard—*Microsoft Windows Configuration*
10. Various Microsoft Documents found at: <http://www.microsoft.com/security/default.msp>
11. *Securing Windows 2000: Step-by-Step*, SANS Institute, V 1.5, July 2001, Jeff Shawgo Editor
12. Naidu, Krishni, *Auditing Windows 2000*, SANS Institute
13. Bragg, Roberta, *Windows 2000 Security*, New Rides, October 2001

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