

## *IT Security Standard:*

# **Windows Base System Configuration**

### **Introduction**

This standard defines the steps needed to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding Windows-based operating systems 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 the management of Microsoft Windows-based operating systems in support of the Bellevue College IT Security Policy. It addresses workstation installations. The general standard applies to both administrative and student systems; all specific exceptions for student computers are identified in the exceptions document.

All Windows-based computers on campus will have the current approved version of the Windows operating system installed unless there are business reasons which prevent this; these non-standard systems will be documented as exceptions.

### **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 workstations covered 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 computer systems, the most significant threats are:

1. Malicious denial of service
2. Maliciously installed viruses, Trojans, and worms (malicious Code)
3. Malicious and/or authorized access, elevating user or system privilege levels
4. Interruption to electrical power or other environmental problems
5. Accidental 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 the Windows workstations is loss of service. This loss of service does have additional 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, 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 more acute on the workstations used on the Student Network. This can include such things as excessive bandwidth use, uses inconsistent with Bellevue College's organizational mission, or uses that are in violation of the applicable Bellevue College Acceptable Use Policies, or federal and/or state law.

## Standard

### A. *System Build and Maintenance*

1. This portion of the standard is not intended to be a complete checklist or comprehensive "best practices document" for building a Microsoft Windows computer, rather this is intended to compliment those types of documents and to speak to the specific security configuration issues at Bellevue College. The purpose is to highlight considerations and requirements in the build processes that have potential security consequences.
2. It should be noted that the items listed in this standard are presented in no particular sequence. In addition, there may be differences in the build between administrative systems and student systems, with lesser restrictions allowed on student systems, using best practices as determined jointly by the members of the IR Information Technology Management Team. Users requiring configurations different from this will request such installations in compliance with the Bellevue College IT Security Standard addressing "*Software Management.*"

### 3. Initial Build

- a. The initial system build will be performed with the computer system either disconnected from the network, if possible, or using a secure network connection. If necessary, it will be attached to "production" networks for installation, but it will not be used on any Bellevue College network in a production capacity until it has been fully built, patched, and security-hardened.
- b. System builds will be performed with a supported version of Microsoft Windows. All security and recommended patch bundles will be applied.
- c. The computer will be configured so that it is included in the antivirus update scheme in accordance with the Bellevue College IT Security Standard addressing "*Virus Protection.*"
- d. File systems on fixed disk devices will be configured as New Technology File System (NTFS); File Allocations Table (FAT), and encrypted file systems will not be used unless permission is granted by the IR Director in charge of the resource. Such permission will be documented to the Bellevue College IT Security Administrator and/or the Dean of Information Resources.
- e. All drive partitions, account policies, group policies, event log and auditing settings, security options, user rights, file permissions, services, and registry settings will be configured and applied in accordance with current best IT practices, as determined by the IR IT Management Team. These decisions will apply to the business and educational application of the systems within the context of all appropriate and applicable Bellevue College IT security standards, including this standard. All services not necessary to support the business use of the computer will be disabled.
- f. The default path, and specifically the systems administrator(s) path, will be verified to assure it is safe and appropriate to the user. Considerations include: which directories are on the path, the sequence of directories, inclusion of the current (dot) directory, and what users may write to directories on the path.
- g. Microsoft Network Client (NetBIOS) will be blocked at the perimeter of the network; limited/controlled access will be granted to the Windows Demilitarized Zone (DMZ).
- h. Modems on workstations will be treated as an exception and documented as such.

- i. The system will be configured to allow installation of software updates without user intervention, but will not allow rebooting without user permission.

#### **4. Software Patches and Updates**

- a. Security patches for OS and application security vulnerabilities will be installed as quickly and safely as possible after their release.
- b. Recommended patches will be regularly installed on the computer unless specific vendor applications prevent installation of current patches. Such cases will be documented as an exception.
- c. Upgrades to new operating systems and application versions will be based on business need. Decisions to upgrade the standard campus operating system for administrative systems will be made by the Information Resources IT Management Team, with the approval of President's staff.

#### **5. Physical Security**

- a. Windows workstations located at a user's desk will be configured with password-protected screen savers that lock the console after no more than thirty minutes.

### **B. System Configuration**

#### **1. Services**

- a. Most of the common "business" services (such as DNS [Domain Name System], 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.

#### **2. Backups and System Recovery**

- a. Bellevue College does not currently backup workstations; staff is expected to store important files on the backup media of their choice.

#### **3. Safe Mode**

- a. In the event of an unexpected reboot, the computer will be configured to complete the boot process without intervention. A short pause will be configured to allow an administrator to interrupt the boot process if needed -- 15 seconds is normally adequate time for this pause.

#### **4. Account Management**

- a. All expectations of the Bellevue College IT Security Standard addressing "Password Management" will be followed. Local System Administration privileges (and responsibilities) will be granted only to authorized IT support personnel. Exceptions may be granted following the procedures in the Bellevue College IT Security Standard addressing "Security Privileges."

### **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: *Password Management*
6. Bellevue College IT Security Standard: *Security Privileges*
7. Bellevue College IT Security Standard: *Software Management*
8. Bellevue College IT Security Standard: *Windows Server Configuration*
9. Bellevue College IT Security Standard: *Virus Protection*
10. SBCTC-IT IT Security Standard—*Microsoft Windows Configuration*
11. Various Microsoft Documents found at: <http://www.microsoft.com/security/default.msp>
12. *Securing Windows 2000: Step-by-Step*, SANS Institute, V 1.5, July 2001, Jeff Shawgo Editor
13. Naidu, Krishna, *Auditing Windows 2000*, SANS Institute
14. Bragg, Roberta, *Windows 2000 Security*, New Rides, October 2001

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