



## *IT Security Standard:*

# **Macintosh Base System Configuration**

### **Introduction**

This standard defines the steps necessary to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding Macintosh-based operating systems deployed on campus. This standard will be reviewed annually or when changes are implemented.

### **Scope**

This standard addresses basic workstation installations and applies to both administrative and student systems. Server installation configurations are addressed in the Bellevue College IT Security Standard addressing "Macintosh Server Configuration."

### **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 (IR), 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 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 unauthorized access, elevated user privilege or system privilege level
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 Macintosh systems is loss of equipment service. This loss of service can 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, 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 greatest on the Student Network. It can include such things as: excessive bandwidth use, uses inconsistent with

Bellevue College's organizational mission, or uses in violation of the applicable Bellevue College acceptable use policies and/or federal and/or state law.

## Standard

### **A. General**

1. Based upon IR recommendations, Bellevue College President's Staff will determine the appropriate Operating System (O/S) version to be installed on Macintosh computers. The following standards are intended to be implemented as closely as possible, dependant on the capabilities of the currently approved O/S.

### **B. System Configuration and Maintenance**

1. This section of the standard is not intended to be a complete checklist or comprehensive "best practices document" for building a Macintosh computer. Rather it is intended to complement those types of documents and to speak to the specific IT security configuration issues at Bellevue College. The purpose is to highlight considerations, requirements, and potential security consequences in the build processes.
2. It should be noted that the items listed herein are not prioritized. Unless otherwise noted, these standards will apply to both workstation and server-class computers. In addition, there will be differences in the build between administrative systems and student systems.

### **3. Initial Configuration**

- a. The initial system configuration will be performed with the computer system disconnected from the network, if possible. 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 configured, updated, and security- hardened.
- b. System installations will be performed with a currently supported version of the Macintosh operating system. All security and recommended updates will be applied.
- c. The computer will be configured to include any antivirus update scheme determined necessary by the systems administrator(s) and the Information Resources Desktop Support Supervisor, in accordance with the Bellevue College IT Security Standard addressing "Virus Protection." All virus updates will be run before putting the system into service.
- d. The computer will be configured to look for automatic updates. The system will be configured to allow installation of software updates without user intervention, but will not allow rebooting without user permission.
- e. Time settings will be configured to set Daylight-Savings time automatically, with the system set to use a Network Time server to acquire the correct time. This can be a local system or the Apple Americas/U.S. site.
- f. File Sharing and Program Linking will be off, unless specifically needed by the end user.
- g. The systems built-in Ethernet will be configured to connect to the Bellevue College network.
- h. Personal firewalls and encrypted hard drives will not be used unless permission is granted by the Director of Computing Services. Such permission will be documented with the Bellevue College IT Security Administrator and/or the Dean of Information Resources. Personal files will be encrypted by the user.
- i. All drive partitions, security options, user rights, file permissions, services, and settings will be configured and applied in accordance with current best IT practices, as determined by the appropriate systems administrator in consultation with IR. 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. Those services necessary to support the educational and/or business use of the computer will be enabled, and will be customized for the end user's needs. Users requiring additional privileges will follow the processes identified in the Bellevue College IT Security Standard addressing "Security Privileges."

#### **4. Security and Maintenance Updates**

- a. Security updates for O/S and application security vulnerabilities will be installed as quickly and safely as possible.
- b. Recommended maintenance updates will be regularly installed on the computer, unless specific applications required by the end user prevent installation because of incompatibility. Exceptions will be documented by IR.
- c. Upgrades to new operating systems and application versions will be based on business and/or educational needs. Decisions to upgrade the standard campus operating system for administrative systems will be processed by the IT Management Team. Requests for exceptions will be sent to the Bellevue College IT Security Administrator and/or the Dean of Information Resources or authorized designee.

#### **5. Services**

- a. Most of the common "business" services have IT security standards defined specifically for them. The computer will be configured with all services needed to accomplish the business or educational use of the computer enabled but unnecessary services will be disabled. A secure Macintosh computer default setup generally has only minimal services enabled.

#### **6. Physical Security**

- a. Macintosh workstations located at a user's desk will be configured with password protection that locks the console after no more than thirty minutes. Requests for exceptions will be processed by the Bellevue College IT Security Administrator and/or the Dean of Information Resources or authorized designee.

#### **7. Backups and System Recovery**

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

### **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 #5150, "*Acceptable Use of Bellevue College Networks and Systems*"
3. Bellevue College Policy #5000, "*Acceptable Use of Bellevue College Computers*"
4. Bellevue College IT Security Standard: *Password Management*
5. Bellevue College IT Security Standard: *Macintosh Server Configuration*
6. Bellevue College IT Security Standard: *Security Privileges*
7. Bellevue College IT Security Standard: *Software Management*
8. SBCTC-IT IT Security Standard—*Microsoft Windows Configuration*
9. Various Apple Security documents found at: <http://www.apple.com/support/security>

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