

IT Security Standard:

Macintosh Server Configuration

Introduction

This standard defines the specific procedural and operating systems configuration elements regarding Macintosh-based servers deployed on campus necessary to implement Bellevue College policy # 5250: Information Technology (IT) Security. This standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard addresses server installations only. General workstation configuration is addressed in the Bellevue College IT Security Standard addressing "Macintosh Base System Configuration." This standard applies to both administrative and student network systems.

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 level or elevated 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,

to some degree, 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 permitted 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. Introduction

1. The Bellevue College IT security standard addressing "Macintosh Base System Configuration" applies to the setup and use of Macintosh server configurations, and all of its expectations will be followed.

B. Initial Build

1. In addition to meeting the "Initial Configuration" requirements listed in the Bellevue College IT security standard addressing "Macintosh Base System Configuration", systems configured as servers will also comply with the following:
 - 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 an adequate pause.

C. Backups and System Recovery

1. System recovery media (tape, CD, floppy, etc.) 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 bare metal" will be available on paper or digital media.
3. The recovery media and documentation will be stored in a location with restricted access control, known to all systems administration staff, the Director of Computing Services, the Bellevue College IT Security Administrator, and/or the Dean of Information Resources (IR). These locations will be reasonably accessible.
4. Backup cycles will vary by computer system, subject to the nature of the computer's task, and the data stored on the computer. The systems administrators for each system will determine the most appropriate backup schedule and scenarios on the systems for which they are responsible.
5. Backup media will be kept on a four-week rotation, with one week being kept at an offsite data storage facility.

D. Account Management

1. All users will adhere to the current Bellevue College IT Security Standard addressing "Password Management." In addition, server configurations will comply with 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 Systems Administration accounts and those noted in the "Password Management Exceptions" document) will not be permitted.
 - c. Accounts are granted for specific business needs, when that need no longer exists, the account will be deactivated or deleted.

E. Elevated Privileges

1. Systems administrators will maintain two accounts: one with normal user privileges and a second with administrator privileges. They will use the unprivileged account for day-to-day work and

execute programs requiring privilege only as needed. In those cases where extended work at elevated privileges cannot be avoided, then authorized systems or network administrators may directly log in to their administrative account.

2. System administration privileges (and responsibilities) will be granted only to authorized IR systems administrators, or authorized designees. On occasion, other trained staff in each of these units will be granted such privileges as necessary to perform their duties.
3. It is accepted that, on occasion, vendors or contractors may—as part of the contracted services—require administrator privileges. These cases will be allowed only with the permission of the Director of the IR unit responsible for the server, and will be documented with the Bellevue College IT Security Administrator.
4. Upon an individual's separation from Information Resources, all privileged access to the Macintosh servers will be terminated. If separating from Bellevue College, access to all Bellevue College systems will be terminated.

F. 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 computer system to high risk environments. Servers exposed to the Internet will be scanned daily; those in more secure environments will be scanned no less than weekly.
2. Basic "health" monitoring will be performed on each server. The systems administration staff will monitor the general health report screen on a regular basis.
3. Web-based system management tools may 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 SSL is highly recommended.
4. Configuration tools restricted to only allow connections from their loopback address will be allowed.

G. Logging and Log Review

1. Logging will be done to a central log host for consolidated storage and processing. If this is done, local logs will also be kept. 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 requiring attention.

H. System Scan/Assessment

1. Systems will receive periodic (no less than once a quarter) network vulnerability scans. Within the limitations of business needs, all vulnerabilities identified will be quickly corrected. 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 the Dean of IR 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 #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: *Security Privileges*
5. Bellevue College IT Security Standard: *Software Management*
6. Bellevue College IT Security Standard: *Macintosh Base System Configuration*
7. Bellevue College IT Security Standard: *Password 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