

IT Security Standard:

Electronic Mail Configuration

Introduction

This standard defines the steps needed to implement Bellevue College policy # 5250: Information Technology (IT) Security with regard to configuring the campus electronic mail (e-mail). The standard will be reviewed annually or when changes are implemented.

Scope

This standard defines specific procedural and configuration elements for management of the Bellevue College electronic mail server software and any special changes required for either the computers on which the server software is installed or on the e-mail client computer systems. Considering the almost exclusive use of Microsoft Outlook in conjunction with a Windows server Active Directory and MS Exchange at Bellevue College, the majority of this standard will focus on security concerns of those specific software applications. Bellevue College cannot enforce compliance with these standards for e-mail clients connecting from home via Microsoft Outlook Web Access, but they can be used as a guideline for home users.

Specific issues regarding appropriate disclosure or protection of information and records retention will not be discussed. For these issues, please see the Bellevue College IT security standards addressing "Data and Information Security" and "Retention of Electronic Records."

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

E-mail has become both core infrastructure and a critical service that enables Bellevue College to communicate within the campus as well as with the outside world in a timely and efficient fashion. Given the high level of dependence on the e-mail, the most significant threats are:

1. Malicious spread of viruses, worms, Trojan horses, etc.
2. Malicious and/or unauthorized use of resources (including spam relays).
3. Denial of service.
4. Malicious forgery and/or spoofing of the sender's address.
5. Malicious and/or unauthorized disclosure of sensitive information.

Given the nature of the asset and the nature of the threat, the primary risk is associated with the spread of malicious content. This can lead to associated risks of: loss of revenue, dissatisfaction of those to whom Bellevue College provides services, interruption of productive work, and loss of reputation.

Secondary to these threats is the potential for inappropriate use of the resource. This can include such things as excessive bandwidth use, uses inconsistent with Bellevue College's organizational mission, or uses that are in violation of Bellevue College Policy #5150, "Acceptable Use of Bellevue College Networks and Systems", Bellevue College Policy #4400, "Acceptable Use of State Resources", and/or state and/or federal law.

Standard

1. General Mail Architecture and Management

- a. Mail servers inside the firewall will relay messages from Bellevue College to the wider Internet through designated mail servers residing on the demilitarized zone (DMZ). Incoming mail, destined for a mail server inside the firewall, will also only be accepted through a mail server on the DMZ.
- b. Establishment of and termination of e-mail accounts are governed by the Bellevue College IT security standard addressing "User Management", and will follow the procedures outlined there. Upon an individual's separation from Bellevue College the mailbox contents for deactivated accounts may be copied from the former employee to a new or existing employee upon request of the Vice President of Human Resources.
- c. All campus users of e-mail accounts will adhere to the Bellevue College IT security standard addressing "E-mail: Guidelines."
- d. E-mail accounts generally will be assigned individually. However, on occasion, shared e-mail accounts may be created to meet a specific unit business purpose.
 - i. Shared e-mail accounts will be set up with a highly complex password, which will not be disseminated to any individual needing to access the account.
 - ii. The shared account will not be used to log into any Bellevue College computing resources.
 - iii. Users will be given permission at their supervisor's request to the shared mailbox through their personal Active Directory accounts and individual e-mail client.
 - iv. When possible, the use of Active Directory security groups will be used to control who is able to access a shared account.
- e. Within Outlook one user may allow another user access to their personal mailbox. While this makes business sense in a few well-defined cases, Bellevue College staff is strongly discouraged from using this feature as it negates privacy safeguards that are in place.
- f. The Bellevue College IT security standard addressing "Non-Employee Access to Bellevue College Systems and Data" governs contractor and consultant access to Bellevue College e-mail and AD accounts. Non-employee users are also required to abide by the various state and Bellevue College policies regarding use of e-mail, principally Bellevue College Policy #5150, "Acceptable Use of Bellevue College Networks and Systems."
- g. Access to the administrative tools for the e-mail service will be restricted to IT support personnel for whom this is a defined part of their duties.
 - i. E-mail administrators may be, from time to time, required to view messages in the message store to investigate or address mail system failures, perform maintenance, or investigate security incidents.

- ii. If e-mail administrators notice evidence of activities that are either unlawful or in violation of policy, they will be required to bring the matter to the attention of the Dean of Information Resources or designee, and/or the IT Security Administrator. Otherwise, the administrators are expected to keep the information confidential.

2. Microsoft Mail Servers

- a. A current, Microsoft supported version of Exchange will be installed on the mail server with its most current security related patches.
- b. On the directory (or drive) containing the Exchange installation, its subdirectories, and the mapisrv.inf file, the following permissions will be set no looser than:

Domain Administrators	Full Control
SYSTEM	Full Control
Users	Read and Execute

- c. To prevent being abused as an SMTP relay for Unsolicited Bulk E-mail (also called UCE, UBE and SPAM), the Internet mail gateway will be configured to not reroute incoming SMTP mail except to other Bellevue College hosts.
- d. Mail servers will be configured to allow encryption/de-encryption of e-mail and any attachments, in accordance with the Bellevue College IT security standard addressing "External Data Transfer."
- e. Up-to-date anti-virus software will scan incoming messages and mailboxes in real time.
- f. Web access to the mail store will be restricted to authenticated users over a 128-bit SSL connection.

3. Mail Client Software

The client is the last in a chain of defenses against e-mail borne attacks. Some of the configuration options specified here can be rigorously enforced, but many rely on the cooperation of the person using the client software.

- a. Exchange accounts will be maintained with strong passwords as required by the Bellevue College IT Security Standard addressing "Password Management."
- b. The e-mail client will be maintained with the most recent security patches.
- c. By default the Outlook client is configured to block "level-one" documents attached to e-mail, as defined in Microsoft's security bulletin Q235309 and the MS Office Assistance website.
 - i. Bellevue College staff will be aware of the dangerous attachment file types.
 - ii. The configuration of the client software may be altered to be more permissive or to have this blocking disabled, depending on the individual user needs.
 - iii. Disabling the level-one attachment check places additional responsibility for careful evaluation of the risks of opening potentially malicious e-mail on the e-mail recipient.
 - iv. When unexpected attachments of the type listed in at the MS Office Assistance website are received they should always be saved to disk and virus-scanned prior to being opened.
- d. Outlook will be configured to use the Microsoft Internet Explorer "Restricted Zone" to minimize the risks associated with malicious executable content, such as ActiveX controls, Java, and JavaScript.
- e. Microsoft Office Macro Protection will be configured to allow execution of signed macros from trusted sources.

- f. Current anti-virus software will be maintained and used on each computer system in accordance with the Bellevue College IT security standard addressing "*Virus Protection*."
- g. Users with administrator rights to the Bellevue College network will use their non-administrator account to access e-mail.

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. *OL2000: Information About the Outlook E-mail Security Update*, <http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q262631>, Microsoft, 2004
2. Pitsenbarger, Bartock, "E- mail Security in the Wake of Recent Malicious Code Incidents," National Security Agency (NSA), Version 2.6, 29 January 2002.
3. Tracy, Jansen, Bisker, *Guidelines on Electronic Mail Security*, National Institute of Standards and Technology (NIST) Special Publication 800-45, 9-2002. Available at: <http://csrc.nist.gov/publications/nistpubs/800-45/sp800-45.pdf>
4. Australian Computer Emergency Response Team (AUSCERT), *Unix Computer Security Checklist*, v1.1, Dec 1995. Available at: <http://csrc.nist.gov/publications/secpubs/index.html>
5. Office Assistance Site, Restricted Attachment file types, <http://office.microsoft.com/en-us/assistance/HA011402971033.aspx>, Microsoft, 2006
6. Bellevue College Policy #4400, *Acceptable Use of State Resources*
7. Bellevue College Policy #5150, *Acceptable Use of Bellevue College Networks and Systems*
8. Bellevue College IT Security Standard: *Data and Information Security*
9. Bellevue College IT Security Standard: *E-mail: Guidelines*
10. Bellevue College IT Security Standard: *Encryption Tools and Protocols*
11. Bellevue College IT Security Standard: *External Data Transfer*
12. Bellevue College IT Security Standard: *Non-employee Access to Bellevue College Systems and Data*
13. Bellevue College IT Security Standard: *Password Management*
14. Bellevue College IT Security Standard: *Retention of Electronic Records*
15. Bellevue College IT Security Standard: *User Management*
16. Bellevue College IT Security Standard: *Virus Protection*

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