



3000 Landerholm Circle SE • Bellevue, WA 98007-6484 • www.bellevuecollege.edu

IT Security Standard:

E-mail Guidelines

Introduction

This standard defines the steps necessary to implement the Bellevue College IT Security Policy within the context of e-mail usage by campus employees. The need for this standard is to assure that the integrity and reliability of the Bellevue College internal networks is not compromised by inappropriate use of the e-mail tools provided to Bellevue College employees. This standard will be reviewed annually or when changes are implemented.

Scope

This standard defines the practices, processes and controls related to using Bellevue College-provided e-mail resources on the Administrative network. While students using e-mail provided through the Academic network are not required to specifically follow some of these guidelines, their general principles still apply to student usage. It is expected that any deviations from this standard for either business necessity or platform implementation constraints will be appropriately documented with the Bellevue College IT Security Administrator.

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, 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 use of Administrative network e-mail accounts at Bellevue College is a vital communication tool in the modern business world. However, e-mail also provides unique opportunities for the introduction of malicious software to the Bellevue College networks and creates risks which can bypass significant security controls traditionally in place to protect those networks. It is through e-mail messages, software included as attachments to e-mail, and related vulnerabilities that most modern threats to network security are introduced.

It is expected that Bellevue College network and systems administrators will take appropriate protective measures to ensure the integrity of the Bellevue College Administrative e-mail systems, in compliance with the Bellevue College IT Security Standard on Electronic Mail Configuration. Despite these precautions, social engineering attacks on network systems take advantage of campus e-mail users who generally do not have sufficient grasp of the related security risks and the potential impact of e-mail attacks on network integrity.

Additionally, a clear standard delineating appropriate use of e-mail on campus becomes a critical factor in assuring the reliability and continued availability of this resource for all users, and in assuring the security of the computing and communications resources under Bellevue College's responsibility.

Given the high level of dependence on the Bellevue College Administrative e-mail system to help campus users accomplish the educational and business missions of the college, the most significant threats are:

1. Accidental and/or malicious destruction or disclosure of critical data
2. Malicious and/or unauthorized access to data and or processes
3. Introduction of malicious software to the Bellevue College network(s)
4. Malicious and/or accidental use of e-mail to perform actions designed to usurp Bellevue College systems and their operation
5. Theft and/or malicious changing of data

Because of the nature of the asset and the nature of the threats, and because of their potential impact on networking resources, all risks associated with the use of e-mail on campus are significant. Any misuse or loss of the networking resources due to misuse of e-mail could put the college instructional and business systems at great risk, with potentially significant loss to Bellevue College.

Standard

General

All user access to Bellevue College e-mail will be governed by the Bellevue College IT Security Standard on E-mail Accounts and other applicable Bellevue College policies and standards. Those Bellevue College users granted e-mail accounts under that standard will use the guidelines in this standard when generating e-mail from their Bellevue College accounts.

The e-mail service at Bellevue College is currently provided through Microsoft Exchange on the e-mail servers, using Microsoft Outlook as the primary e-mail client. Procedures identified in this standard reflect the use of those software tools.

Campus users should contact the Help Desk through Request Center or by phone (at x4357) if they are uncertain regarding the appropriate use of e-mail, have questions concerning any of the e-mail policies and/or standards, or require assistance with technical problems related to campus e-mail resources.

Distribution Lists

Distribution lists are groupings of e-mail addresses which allow a single e-mail to be sent to many people at once. Distribution lists should not be used merely because it's quick and convenient for the sender; it can be very inconvenient for many recipients. Use of the Bellevue College distribution lists always requires good judgment.

Personal Distribution Lists

Campus e-mail users are encouraged to make use of personal distribution lists to organize those groups of e-mail addresses to which they send mail frequently. This is done within the user's Contacts list. Personal distribution lists are only visible and available to the individual user who created them within their own e-mail account.

Public Distribution Lists

Public distribution lists are visible and available to all e-mail users using Bellevue College Administrative e-mail accounts. They have been created to provide all campus users standardized logical groupings of e-mail addresses. Use of the Bellevue College public distribution lists always requires good user judgment. Those misusing Bellevue College public distribution lists will be warned and asked to modify their behavior.

These lists reflect groups of users on campus (such as “Macintosh Users”), users within units on campus (such as “Records Coordinators”), users assigned to temporary task forces (such as “Title III Task Force”) or committees (such as “Innovation Grant Committee”), or users with similar interests (such as “Diversity Caucus”). Multiple distribution lists may be combined in a single e-mail, as can multiple individual recipients.

1. Public distribution lists can only be created by e-mail server administrators. A request for creation of a public distribution list should be made to Information Resources through Request Center.
 - a. Establishing a public distribution list requires administrative approval. While a written request is not required, Information Resources support personnel will verify the need for and the appropriate name of a public distribution list with an administrator prior to creation.
 - b. There must be a valid business purpose for a public distribution list.
 - c. The requesting administrator for a public distribution list must designate someone to be responsible for advising Information Resources of changes and ensuring its accuracy (a list “owner”) before the list can be created.
 - d. The owner of a public distribution list will keep the distribution list current and will “clean up” the list at least every six months, removing references to accounts of individuals no longer authorized to receive mail sent to the list. This includes removal of individuals from the list membership who are no longer at the college.
 - e. This ongoing list maintenance is required to reduce the amount of unnecessary e-mail stored on Bellevue College servers and to reduce the number of undeliverable e-mails which occur when a recipient’s mailbox no longer exists.
2. Names of distribution lists appear alphabetically, in **bold type**, throughout the Exchange Global Address List.
 - a. To see a listing containing only current public distribution lists, open the Address book, click on the “Show Names from the:” drop-down menu in the upper right corner, and choose “All Groups”.
 - b. To see a dialogue box identifying the “owner” of a public distribution list and which e-mail recipients are included in the list, double-click on the list name after it has been added to the message address.
3. There are three special “broadcast” public distribution lists which include most campus e-mail users. In order to allow recipients to distinguish messages to these special lists from personal messages, all require a special designation in square brackets within the subject line:
 - a. **All Bellevue College-Official**
 - i. The subject line for “All BC-Official” messages must begin with the word “Official” in square brackets: **[Official]**.
 - ii. The “All BC-Official” distribution list includes all Bellevue College e-mail recipients; campus users may not be removed from the list.
 - iii. The “All-BC-Official” distribution list may only be used for official college messages that *all* employees *need to know*, rather than messages they might be interested in.
 1. Examples include: College Issues day announcements, campus closure notices, or messages to the entire campus from the President and/or Deans/VPs.
 - iv. Recipients should never use a “Reply to All” response to any “All BC-Official” messages. Any needed reply should be directed to the individual sending the message.

- v. The “All BC-Official” distribution list is the only public distribution list which requires approval of the sender’s Dean/VP before use. This approval authority may be delegated by the Dean/VP.
- vi. “All BC-Official” should not be used for announcements to the campus of personnel changes (hiring, separations, retirements, etc.). “All BC-FYI” is the more appropriate forum except in the most significant cases.

b. All BC-FYI

- i. The subject line for “All BC-FYI” messages must start with the letters “FYI” in square brackets: **[FYI]**.
- ii. FYI is an acronym for “For Your Information.” The “All BC-FYI” distribution list includes most Bellevue College e-mail users, but is optional. Messages in this category are for college related information in which most recipients might be interested.
 - 1. Examples include: announcements for campus events, information of general interest, special requests to the college community.
- iii. Campus users may submit a request to Request Center asking to be removed from the “All BC-FYI” distribution list.
- iv. Campus users are required to consider the importance of the message to the recipients, not the sender, before sending to the “All BC-FYI” distribution list.
 - 1. This distribution list should only be used if the message will be of interest to the large majority of recipients. If not, a more closely targeted distribution list, or list of individuals should be used.
- v. All e-mail messages sent to the “All BC-FYI” distribution list must be related to college business.
 - 1. For instance, campus club fund raiser announcements are acceptable, while Girl Scout cookies or TV For Sale are not.
- vi. No more than two [FYI] e-mail notices should be sent to the campus regarding a single event.
 - 1. Large campus events may have two: one, an advance notice a week or two before, and the second a reminder the day before or day of the event.
 - 2. Routine events should have only one notice.
- vii. Campus users should never use a “Reply to All” response to any “All BC-FYI” messages. Any needed reply should be directed to the individual sending the message.
- viii. “All BC-FYI” is not appropriate as a forum for personal or political statements.

c. All BC-PFD

- i. The subject line for “All BC-PFD” messages must start with the letters “PFD” in square brackets: **[PFD]**.
- ii. PFD is an acronym for “Public Forum Dialogue.” The “All BC-PFD” distribution list includes most campus e-mail users, but is optional. This category of message is for dialogue about important campus issues that will be of interest to many campus employees.
 - 1. Examples include conversations about students as customers, smoking policy, grade inflation, or any other discussions important to the college as a community.

- iii. Campus users may submit a request to Request Center asking to be removed from the “All BC-PFD” distribution list.
- iv. Campus users are required to consider the importance of the message to the recipients, not the sender, before sending to the “All BC-PFD” distribution list.
 - 1. This distribution list should only be used if the message will be of interest to the majority of recipients. If not, a more closely targeted distribution list, or list of individuals should be used.
- v. Campus users are expected to be considerate of all recipients in limiting the number of messages sent to the “All BC-PFD” distribution list.
 - 1. Messages to “All BC-PFD” should add to or amplify the dialogue. Simply responding “I agree” is not worth the imposition on everyone’s time and Inbox.
 - 2. Users should collect their thoughts into one well-crafted message rather than several rapid fire “and another thing ...” messages.
- vi. Within the above considerations, “All BC-PFD” messages ARE intended for “Reply to All” responses.

Using Bellevue College e-mail for soliciting contributions

Using any Bellevue College resource, including the Bellevue College e-mail system, for commercial purposes—including advertising or selling—is strictly prohibited by state Ethics guidelines and the Bellevue College policy on the Acceptable Use of State Resources. However, the use of such Bellevue College resources for fundraising or for donations to charitable organizations is specifically allowed, if authorized by the President of the college.

Guidelines

The following guidelines have been created to help the college community to clearly understand what an appropriate fundraising solicitation is and what may be an inappropriate commercial solicitation when using the Bellevue College e-mail system and the All-BC distribution lists.

1. For the purposes of these guidelines, both requests for charitable donations and/or selling as a part of an authorized campus fund-raising effort will be considered “fundraising.”
2. These guidelines will be followed in all cases where Bellevue College e-mail is used. These guidelines do not govern fundraising solicitations through means other than e-mail.
3. All e-mail solicitations to the college as part of any fundraising effort on campus which follow all aspects of these guidelines may be sent to the campus without prior approval from the college President.
4. When composing an e-mail for fundraising purposes, the term [Fundraising] must be entered into the subject line preceding the description of the e-mail’s topic, surrounded by square brackets (as illustrated). This is in addition to the [FYI] subject line requirement, i.e: [FYI] [Fundraising]...
5. All [Fundraising] solicitations through Bellevue College e-mail involving a student organization or effort must be approved by and originate from the Student Programs office. All other solicitations may be approved by the originating unit’s administrator.
6. E-mail solicitations may only be made using the *All BC-FYI* distribution list. Use of the *All-BC-Official* distribution list is strictly prohibited.
7. [Fundraising] solicitations using *All BC-FYI* may only be made for efforts that directly support a campus entity. There must be a direct benefit to the college community as a result of the fundraising.

8. [Fundraising] solicitations may not be made using the Bellevue College e-mail system for any outside entity, even if Bellevue College facilities are being used to host the organization or an associated event.
9. No more than three e-mail notices may be distributed to the campus for any single fundraising effort. In addition, no more than one e-mail notice during any single work-week may be sent.
10. Any reference within a [Fundraising] e-mail to any tax benefits or potential tax benefits related to a purchase or contribution is strictly prohibited.

Exceptions

The college President must approve in advance any fundraising solicitations using Bellevue College-owned e-mail systems that do not fall within these guidelines and/or any exception to these requirements.

Expectations for e-mail usage

As with all equipment and tools provided on campus, Bellevue College e-mail users are expected to use e-mail appropriately within the expectations of the Bellevue College policy on the Acceptable Use of State Resources. In addition the following expectations should be understood:

Appropriate Audience

Every e-mail message should be sent to everyone who wants or needs it, and to no one who doesn't. Messages should be carefully targeted to recipients.

Descriptive "Subject" line

Careful consideration should be used to make the "Subject" line in an e-mail appropriate and descriptive. Recipients should be able to easily determine if they are interested in reading without opening the message.

E-mail management

Consistent effort to manage e-mail is extremely important. Each campus user has a responsibility to control the impact their e-mail has on the Bellevue College systems. In managing the campus e-mail servers, Information Resources sets 300 MB storage space limits on all Bellevue College administrative e-mail accounts. Campus users whose mailbox exceeds the set limits will be notified and asked to bring their volume of stored e-mail into compliance.

The campus Help Desk can assist users in managing e-mail mailboxes. Practices that can be undertaken to limit e-mail volumes on the Bellevue College servers include:

1. Deleting unwanted e-mail messages to minimize mailbox volumes.
 - a. Campus users should routinely review their e-mail and delete unwanted messages.
 - b. Voice mail is also stored on the e-mail server, so it is critical that unwanted voice-mail be deleted as well. Voice-mail messages are much larger than most e-mail messages.
2. Creating personal e-mail folders located on the local hard drive to store saved messages.
3. Setting e-mail "rules" and filters so that incoming mail will automatically be moved to various personal e-mail folders.
 - a. For example, all [FYI] and/or [PDF] mail may be automatically directed to separate folders, stored on the local hard drive (thus freeing up server space). They then can be read when time is available, but do not clutter up the Inbox or impact space limitations in the meantime.

Security/Confidentiality

Bellevue College e-mail accounts are tied to Bellevue College Administrative network accounts, allowing control of both log-in and e-mail accounts by the same password.

Passwords are used to prevent unauthorized access or use of another user's e-mail account and to prevent non-recipients from reading another user's e-mail.

However, passwords alone do not mitigate the high risk to Bellevue College resources created through e-mail use. Campus users must always be vigilant and security-conscious with regard to their e-mail.

1. Bellevue College users must protect the passwords for their e-mail accounts in accordance with the Bellevue College IT Security Standard on Password Management. This includes prohibitions on sharing their personal log-in or e-mail passwords.
2. Campus users must never leave their work area without securing any computer being used. A common way to obtain malicious access to an e-mail account is for someone to simply sit at a computer that is already logged into e-mail.
3. While Bellevue College's e-mail system is encrypted to help prevent messages being compromised in transmission, e-mail should not be used for sensitive or confidential messages sent to a non-Bellevue College e-mail address.
4. Because most attacks against computer networks using e-mail are made possible through an e-mail attachment, it is best to avoid the use of attachments unnecessarily.
 - a. Whenever possible, include all of the information within the message rather than send an attachment. Most text can be copied from a document and pasted into an e-mail message.
 - b. Bellevue College users should never open attachments to e-mails from senders they do not know.
5. Because of the current state of malicious attacks through e-mail, campus users should always be skeptical of e-mails that contain hyperlinks and/or graphics, as well. The basic rule-of-thumb is to delete without opening any e-mail from an unknown source or which appears suspicious.

Disclosure

College practices related to e-mail will observe the privacy and confidentiality of Bellevue College e-mail accounts to the extent allowed by state and federal law and by college policy. However, state law mandates that e-mail created with or mailed to Bellevue College e-mail accounts are the property of the institution and subject to public disclosure.

1. Copies of all e-mail sent or received on campus are housed on the Bellevue College e-mail servers. Access to those messages may continue to exist for an extended period of time even after a user has deleted them from within their Outlook client.
2. Individual e-mail messages may be released to auditors or outside law enforcement agencies after an appropriate request to review. Bellevue College will cooperate fully in any official investigation by an outside agency.
3. If access to e-mail messages, accounts and systems is required, the Human Resources office will be responsible for providing the necessary information.

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 Dean of Student Services (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 Acceptable Use of State Resources Policy
2. Bellevue College Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems Policy
3. Bellevue College Acceptable Use of Bellevue College Computers Policy
4. Bellevue College E-mail Usage Policy
5. Bellevue College IT Security Standard: Electronic Mail Configuration
6. Bellevue College IT Security Standard: E-mail Accounts
7. Bellevue College IT Security Standard: Password Management
8. Bellevue College IT Security web site: <https://go.mybcc.net/sites/itsecurity>

Effective Date:	July 12, 2005
Date Last Modified:	July 10, 2009