



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

IT Security Standard:

E-mail Accounts

Introduction

This standard defines the steps needed to implement the Bellevue College IT Security Policy for management of all Bellevue College-based e-mail accounts used by staff, faculty, students, and authorized non-employees. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines the specific procedures for creating and managing e-mail accounts on the Bellevue College e-mail servers in support of the Bellevue College IT Security Policy. Its general tenets apply to all e-mail accounts on either the administrative or academic e-mails systems in place at the college.

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

Bellevue College uses e-mail for the vast majority of its communications. Bellevue College policies carefully govern the use of e-mail accounts in accordance with state law. While not creating a direct threat to the integrity of the Bellevue College network systems, e-mail is still the most common point of entry to the network for malicious and destructive applications. As such, careful consideration in the granting of e-mail accounts and their associated domain log-in accounts is a critical factor in assuring the security of the computing and communications resources under Bellevue College's responsibility. A significant compromise to e-mail security could put the college instructional and business systems at great risk.

Bellevue College, as an institution of higher learning, also has important legal and moral responsibilities with regard to the dissemination of information, particularly information classified as private. A part of this responsibility is to limit access to such information and its methods of distribution, including via e-mail, to those individuals authorized to manage such data. Finally, the careful use and management of the e-mail accounts associated with Bellevue College is a critical factor in how the college participates in the world community. Preventing potential misuse of Bellevue College resources to distribute harmful files to the wider Net is as important as preventing harmful files from entering Bellevue College by this path.

Given these responsibilities, the most significant threats are:

1. Theft and/or malicious manipulation of data via e-mail

2. Fraudulent use and/or theft of e-mail services
3. Introduction of malicious executable code into Bellevue College network via e-mail
4. Use of e-mail to inappropriately disclose private information

Given the nature of the asset and the nature of the threat, all risks associated with Bellevue College-based e-mail accounts are very significant and could cause significant loss to Bellevue College.

Standard

The use of e-mail at Bellevue College is generally necessary for employees to accomplish work duties. In addition, other users providing services to the campus may have a need to communicate in this manner, as well. All users of Bellevue College e-mail systems have a responsibility for how this resource is used. This standard identifies the types of users on campus who may be authorized to use Bellevue College e-mail accounts, the campus units responsible for managing and providing access to those services, and the mechanisms in place to gain authorization to utilize this resource. Additional information regarding management of user accounts at Bellevue College can be found in the IT Security Standard on User Management.

Responsibilities

Information Resources has responsibility for the creation and management of the Administrative network and its associated e-mail system, which houses the primary log-in and e-mail accounts used to support the daily operations of the campus. In addition, IR has responsibility for the creation and management of the Academic network e-mail system and accounts. This network and associated e-mail systems provide the e-mail accounts assigned to students in support of their academic studies and to faculty and support staff in direct support of academic curriculum delivery.

The Dean of Information Resources and/or his delegates will assign responsibility for the creation and management of all Bellevue College network e-mail systems and accounts to qualified IT support personnel as needed to fulfill the responsibilities identified in this standard.

Accounts

Because a Bellevue College network domain account is required as a basis for creation of e-mail accounts at Bellevue College, all users must follow the procedures outlined in the Acceptable Use of the Bellevue College Networks and Bellevue College Data Management Systems Policy to obtain a log-in and e-mail account. All log-in and e-mail accounts will be created, maintained and deleted by authorized IR support personnel.

Employee e-mail accounts

If any individual is performing work which is directly compensated by the college and is classified as an employee by the Bellevue College Human Resources office, this section of the standard applies; employees therefore may be full or part-time. Before using the Bellevue College network, employees must formally request permission for a log-in/e-mail/voice mail account.

1. The **Bellevue College Network Account and E-mail Request form** must be filled out, providing all applicable information.
 - a. The signature of the individual requesting the account is required.
 - b. The approving signature of the administrator to whom the individual reports is required.
2. In the event of changes to Bellevue College policies, standards or procedures, the Dean of Information Resources may require Bellevue College account holders to periodically submit an updated Bellevue College Network Account and E-mail Request form.
3. Completed forms must be routed to the technical support Help Desk for processing.
4. The completed Bellevue College Network Account and E-mail Request Form will be maintained on file in a secure location in IR.

Non-employee e-mail accounts

Non-employees may, under some circumstances, be granted permission to use the Bellevue College network in performing some service for the college. Non-employees may also be granted

permission to have a Bellevue College e-mail account. These privileges for non-employees are not mutually inclusive. In other words, a non-employee may have a log-in account, but not an e-mail account.

Non-employees may include volunteers on campus, vendors, employees of co-located agencies, non-paid student interns, etc. All individuals not classified by the Bellevue College Human Resources office as employees who need access to either the Bellevue College networks or a Bellevue College-provided e-mail account must formally request permission for a non-employee log-in/e-mail/voice mail account using the following guidelines:

1. The request for any type of non-employee e-mail account must be generated and approved by the administrator responsible for overseeing the services being provided by the non-employee.
2. This is accomplished by completing and signing the **Bellevue College Network Account and E-mail Request Form** providing the applicable information.
 - a. This form must be routed to the Help Desk for processing by the IR staff authorized to create and maintain accounts on the administrative network.
3. Non-employee e-mail accounts will only be active during the specific period of time the individual is performing a service to Bellevue College which requires such an account. An expiration date for non-employee accounts will be noted on the Bellevue College Network Account and E-mail Request Form. If a non-employee requires account access beyond the expiration date the approving supervisor will notify IR of the need.
4. The only exception to this requirement are those e-mail accounts classified as “emeritus” or “student”, which must be requested and approved as described below.

Emeritus e-mail accounts

Staff and faculty members who have been employed for an extended period of time at Bellevue College may be granted an “emeritus” e-mail account for use after their official Bellevue College relationship has ended.

1. Emeritus e-mail accounts must be requested by the individual desiring such access through the Human Resources office.
2. The form at **Appendix B of this standard** will be completed and approved, then routed to IR through the Help Desk before an emeritus e-mail account will be created.
3. Emeritus e-mail accounts must be approved in advance by the Vice President for Human Resources.
4. Emeritus e-mail accounts will be created and housed on the Administrative network e-mail server system.
5. The word “Emeritus” in parenthesis will be displayed as part of the e-mail name.
6. Emeritus e-mail accounts will be included in the All BC-Official, All BC-FYI, and ALL BC-PFD distribution lists unless requested otherwise.
7. Emeritus e-mail accounts will have a limited mailbox size of 330 MB.
8. Emeritus e-mail accounts with no activity for a period of one year may be removed without further notice.
9. Upon creation of an emeritus e-mail account, the user’s official Bellevue College account will be deleted. Users should back up any important data from that account before requesting an emeritus e-mail account.
10. Users of emeritus e-mail accounts must continue to abide by the policies regarding the Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems, the Acceptable Use of State Resources and the Acceptable Use of Bellevue College Computers.
11. Users of emeritus e-mail accounts are not relieved of any requirements to continue to protect the confidentiality of college data in accordance with the Family Education Rights and Privacy Act (FERPA) and Washington State Ethics Law.
12. Users of emeritus e-mail accounts continue to be bound by the Bellevue College policies and guidelines related to the use of electronic messaging systems.

Student e-mail accounts

Student e-mail accounts are housed on the Academic server systems and have no access to the Administrative networking domain. Because of this, a formal written request and approval process for creating student accounts is not required.

1. The method for creation of student user log-in/e-mail accounts for use on the Academic network will be at the discretion of the Academic Network Administrator, with the approval of the Director of Computing Services. Accounts may be requested by students and processed strictly by electronic means, if feasible.
2. Students are expected to abide by all expectations, responsibilities and guidelines of the Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems Policy, any other applicable Bellevue College policies, standards and procedures and applicable State and Federal laws and rules.
3. A student e-mail account may not be created until the Academic Network Administrator has ensured that the student has read and agreed with those policies.
4. This may be done with the use of a Web form requiring electronic acknowledgement by the student when requesting an account (using the information contained in the **Bellevue College Network Account and E-mail Request form**).
5. Log-in banners that must be acknowledged before use of Academic network or computing resources, containing the same textual information, may also be used.
6. Information Resources will also maintain an electronically accessible copy of this policy and any related procedures and standards on the Academic Support web site, and a printed copy in the Open Lab in N250 on the main campus.
7. Student e-mail accounts will only be activated during the school year for which a student is registered.
8. All student e-mail accounts will be disabled and purged of all messages at the end of Summer quarter each academic year.

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 log-in 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. Acceptable Use of the Bellevue College Network and Bellevue College Data Management System Policy
2. Acceptable Use of State Resources Policy
3. Acceptable Use of Bellevue College Computers Policy
4. Bellevue College IT Security Standard: Non-Employee Access to Bellevue College Systems
5. Bellevue College IT Security Standard: User Management
6. Family Education Rights and Privacy Act (FERPA)
7. RCW 42.17 -- Washington State Ethics Law

Effective Date: March 2004
Date Last Modified: July 10, 2009