

IT Security Standard:

E-mail: Mass Mailing

Introduction

This standard defines the steps needed to implement Bellevue College policy # 5250: *Information Technology (IT) Security* regarding the use of Bellevue College technical resources to send unsolicited e-mail to multiple recipients. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard applies to all Bellevue College users and is relevant to any e-mail generated using Bellevue College servers and applications sent to a large block of e-mail addresses simultaneously.

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

E-mail is a primary medium for communication between Bellevue College users, whether they are faculty, staff, students or guest users of the technical resources on campus. The use of Bellevue College e-mail resources (servers, network infrastructure and computers) is a vital service supporting both the business and educational missions of the college.

A primary concern generating the need for this standard is that of placing a significant additional demand on the Bellevue College resources which support the processing and storage of e-mail on campus. In effect, too great a demand for e-mail processing can have the effect of limiting all other network activities—essentially shutting down critical systems and services.

Given the impact of violations of this standard, the most significant threats are:

1. Denial of service resulting from exceeding system capacity.
2. Malicious and/or inappropriate use of resources.
3. Loss of institutional prestige within the community.

Considering the nature of the asset and the nature of the threats listed, the main risks associated with sending mass e-mailings from Bellevue College servers are denial of services. All of these threats have additional associated risks of: loss of revenue, dissatisfaction of those to whom Bellevue College provides services, interruption of productive work, and loss of reputation.

Standard

A. Business and Marketing Uses

1. Communication with students, potential students, and others through e-mail is a vital tool for many of the business operations at Bellevue College, and can be an effective means to reach those individuals with business and marketing information.
2. However, the practice of sending a single message to a large number of e-mail addresses simultaneously, sometimes called mass or bulk e-mailing, must be infrequent and carefully governed so that the resources providing e-mail services on campus (networks, servers, computers) are not impacted severely enough to prevent their normal day-to-day operations.
3. In addition, many individuals consider ANY unsolicited mass e-mail to be “spam” (defined as unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups), so the practice of mass e-mailing subjects Bellevue College to potential public embarrassment and a negative community image if misused—thus negating any promotional or communicative benefit to the institution derived from allowing mass e-mailing.
4. Mass e-mails may be sent using Bellevue College computing resources only under the following conditions:
 - a. The e-mail may only be sent in relation to Bellevue College-sponsored activities, not on the behalf of any outside organization, even if the event is being held on a Bellevue College campus;
 - b. The e-mail must be approved by a college dean or vice-president;
 - c. The e-mail must include an “opt-out” reply mechanism for the recipient; and
 - d. The e-mail must provide a return address for comments and questions.

B. Permitted Exception

1. This standard is not intended to restrict the use of e-mail sent to students during specific, on-going interactions regarding their attendance at the college, such as enrollment, financial aid, etc.

C. Specific Prohibitions

1. Nothing in this standard permits sending e-mail for the purpose of promoting real property, goods, or services for sale or lease under any of the following circumstances, all of which are state law violations:
 - a. Sending an e-mail message which misrepresents any information in identifying the point of origin or transmission path of that mail.
 - b. Sending an e-mail message which contains false or misleading information in the subject line.
 - c. Sending an e-mail message which uses a third party’s Internet address without permission.
2. No lists of e-mail addresses collected or retained by Bellevue College may be sold, loaned, leased or given to any organization outside of Bellevue College.

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. RCW 19.190.010-070
2. Definition of "spam" from <http://www.dictionary.com>
3. Bellevue College Policy #4400: Acceptable Use of State Resources
4. Bellevue College Policy #5000: Acceptable Use of Bellevue College Computers
5. Bellevue College Policy #5150, Acceptable Use of Bellevue College Networks and Systems
6. Bellevue College Policy #5250: Information Technology (IT) Security

Effective Date: May 2006
Date Last Modified: April 12, 2009