

IT Security Standard:

Data and Information Security

Introduction

This standard addresses issues related to implementing Bellevue College policy # 5250: Information Technology (IT) Security with regard to protecting sensitive information that is collected, stored, transported or manipulated in an electronic form that is accessible through the Internet and the world-wide web. This standard supplements the requirements of Bellevue College policy #2550, addressing "Federal Privacy Act: Disclosure of Social Security Numbers" and policy # 2600, "Family Education Rights and Privacy Act: Disclosure of Student Information", and will be reviewed on an annual basis, or when changes are implemented.

Scope

This standard applies to disclosure of any data or information collected in electronic form at Bellevue College, and is intended to reduce the risks associated with unauthorized access to, disclosure of, or destruction of Bellevue College-controlled data. It is the responsibility of all Bellevue College technology users to comply with this standard, with all applicable Bellevue College policies and standards, and with local, state and/or federal laws regulating privacy and information dissemination.

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

Unauthorized access by any means to sensitive Bellevue College data is an extremely serious security issue. However, because the manipulation and storage of this data is increasingly in electronic format, and the technology used to accomplish these tasks are increasingly network, web and internet based, data that was previously able to be easily secured is now exposed to potential disclosure to unauthorized individuals on a world-wide basis. Balancing accessibility to and security of sensitive data is becoming the most difficult issue with regard to IT security. Limiting access to the data stored, maintained and shared by Bellevue College networks and computer to only those authorized is therefore a high security priority.

The most significant risks related to protection of Web-accessible data and information are:

1. Malicious destruction, modification and/or disclosure of critical protected data.
2. Unauthorized access to data, allowing theft of information, fraud or misuse.
3. Accidental modification or destruction of data by those authorized.

The primary risk associated with failure to comply with this standard is the unauthorized disclosure of information Bellevue College is required to protect, including the personal information of students or staff, and information which could lead to compromise of the network and its accounts. Problems resulting from this kind of disclosure include: loss of the network itself, loss of revenue, loss of reputation and the potential for litigation. Such disclosure can also be a violation of local, state and/or federal law.

Standard

A. Introduction

1. This standard is not intended to limit access to protected information and data by authorized users, nor is it the purpose of this standard to make each campus user an expert on the various public disclosure and confidentiality laws. Rather, its purpose is to heighten the awareness of each individual regarding the protections required for the data they handle on a daily basis as part of their association with Bellevue College.
2. Protection of sensitive data collected and used at Bellevue College is a primary purpose for implementing security measures governing the information technology resources on campus. Bellevue College is required by law to protect many pieces of the data collected on a daily basis to support the business of the college.
3. Historically, access to sensitive data in printed or electronic format by individuals was very limited. Now it is available through ubiquitous internet networking resources to all employees. This easy accessibility to the data tends to decrease the caution used by campus users to ensure its security. Campus users sometimes take appropriate precautions to protect printed copies of data, but disregard the protection of exactly the same information in electronic format.
4. Appropriate data security protects both electronic and printed data and includes the full life cycle of the data, from creation through destruction. Sensitive and confidential data collected and used at Bellevue College will be protected, no matter what form it has or how it is accessed.

B. Categories of Electronic Data

1. Identifying categories within this standard does not imply a liberty on the part of an individual to disclose data to the public outside of the procedures prescribed under the open public records and meetings laws. Electronic data is classified as follows:

a. Public Information

This is information and/or data for which there is no state or federal law restricting disclosure and/or release to the public. While it does not need special protection from unauthorized disclosure, it does need protection from unauthorized changes that alter the information. This includes all information that is already in the public view, but does not include public records that are exempted from public access according to RCW 42.17.310 and WAC 132H-169-070.

b. Sensitive Information

This is information that may ultimately be defined as a public record and able to be disclosed, but will be carefully protected prior to being released through the campus disclosure process. This might include financials, payroll-personnel, operating procedures, as well as basic computer, network and security configurations.

c. Confidential Information

This is information that cannot be released to the public, being specifically protected by state or federal law. Confidential information should deliberately and carefully be protected from disclosure, and generally includes:

- i. Personal information about individuals, regardless of how that information is obtained.

- ii. Information concerning employee payroll and personnel records.
- iii. IT security information that, if released, could jeopardize the integrity of data or result in fraud, unauthorized disclosure, or modification of information.

d. Information Requiring Special Handling

Information requiring special handling is confidential information for which additional protections need to be in place. This will include information such as student information, personnel health records, credit card information, and other similar data. This includes, but is not limited to:

- i. Information for which either state or Federal laws or regulations require protection or dictate particular handling requirements, for example, the Family Education Rights and Privacy Act (FERPA) or Health Information Portability and Accountability Act (HIPAA).
- ii. Information that is covered by a contract or agreement in which specific and strict handling requirements are set forth.
- iii. Information for which serious consequences can arise from unauthorized disclosure ranging from life threatening action to legal sanctions.

C. Accessibility to Electronic Data

1. Electronic data is subject to the same privacy restrictions as non-electronic information and requires the same protections. Information disseminated through any internet-accessible medium will conform to the Washington state Department of Information Services (DIS) and the Information Services Board (ISB) "Public Records Privacy Protection" policy, which in turn implements Executive Order 00-03, "Public Records Privacy Protections." These specific requirements also apply:

a. Web

All Bellevue College web sites will be in compliance with the Bellevue College IT security standard addressing "Web Servers." Public information posted on a Bellevue College web site shall be reviewed and approved for release in the same manner as other public dissemination of official memos, reports or other official non-electronic data and information. Sensitive and confidential information accessible through a web site will be password protected and will not be stored or posted in the same directories as public information.

b. E-mail

E-mail sent to internal administrative Bellevue College addresses is considered secure and may be used with discretion to disseminate confidential and sensitive information. Confidential and sensitive information will not be included in any e-mail which is addressed to an external e-mail address or to a Bellevue College student e-mail address.

c. Blogs

Blogging sites are a specialized type of web site and are therefore covered under the requirements identified under "Web", above. However, because of the spontaneous nature of many blogging interactions, special care and caution should be taken by campus users to ensure that confidential and sensitive information is never included in a blog posting, whether the hosting blog site is internal or external to Bellevue College.

d. Instant Messaging

Because the sites hosting instant messaging may or may not be external to Bellevue College, maintaining security over information distributed in that manner cannot be guaranteed. Therefore, confidential and sensitive data should never be included in any instant messaging posting, no matter whether the recipient is another Bellevue College user or not. If such information needs to be exchanged between Bellevue College recipients, e-mail should be used.

e. Podcast

Confidential or sensitive information will not be posted as part of any Podcast or as part of any web site, page or file transfer site supporting Podcasting. This restriction applies whether the hosting site is internal or external to Bellevue College.

D. Storage of Electronic Data

1. Data can be stored in a variety of forms, depending on the usage needs. There are also differences in how data is stored on campus by individual users and how Information Resources is required to store data for which they are responsible. The most common formats are: on a computer system's disk drives or network drives, on various backup media (tape, floppy, CD, USB), and on printed reports.

a. General Storage

- i. Electronic data retained by the institution in compliance with Bellevue College Policy #6900, "Records Storage and Disposal" will not be stored on any internet-accessible location, but will be moved to off-line media, such as disk or tape.
- ii. Electronic data stored on any media will be secured commensurate with its level of confidentiality or value. Some data that is labeled confidential might, for example, require encryption and/or storage only within a database.
- iii. Backup media must be stored in such a way as to assure both its magnetic integrity, but also its physical security.
- iv. Hard copy reports of data created for internal use at the Bellevue College will be protected commensurate with the sensitivity of the data they contain. When hard copies are no longer needed, they should be disposed of properly. Printouts that contain any sensitive or confidential information will be shredded.

b. Information Resources

- i. IR support personnel will rotate three sets of system backup tapes to an off-site data storage facility. This rotation will keep one set of backup tapes available on campus and two sets off-site at any given time. The data storage vendor will demonstrate that:
 - The company mitigates environmental hazards (flood, earthquake, fire),
 - The company and its employees are bonded,
 - Data is stored by the company in a climate-controlled facility, and
 - The company observes reasonable, up-to-date security practices in protecting their customers' data.

E. Destruction of Electronic Data

1. Electronic data must be retained in accordance with Bellevue College policy #6900, "Records Storage and Disposal", commensurate with the type of data it is. When a data storage medium, or the data on the medium, has reached its end of life, it will be disposed of properly.
 - a. Destruction of electronic data will comply with the Bellevue College IT Security Standard addressing "Media Disposal", which defines specific procedural and configuration elements for disposal of media used to store potentially sensitive data. This media may include magnetic, optical, and other electronic media.
 - b. For printed media such as paper, microfilm, and fiche, the "Media Disposal" Standard may be selectively applied to media specifically containing sensitive data.

F. Security Breach Notification

1. Failure to maintain, secure or destroy electronic copies of information that is sensitive, confidential, or requires special handling as described in this standard is a serious matter, and may be a violation of state law. If such failure occurs, the processes described in the Bellevue College "Security Breach Notification" policy will be followed and all mandated notifications made.

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

2. RCW 40.14
3. RCW 42.17.310
4. WAC 132H-169-070
5. Bellevue College Policy #1500 – Access to Public Records
6. Bellevue College Policy #2550 – Federal Privacy Act: Disclosure of Social Security Numbers
7. Bellevue College Policy #2600 – Family Education Rights and Privacy Act: Disclosure Of Student Information
8. Bellevue College Policy #5250 – Information Technology (IT) Security
9. Bellevue College Policy #6900 – Records Storage and Disposal
10. Bellevue College Policy #5260 – Security Breach Notification
11. Bellevue College IT Security Standard: Database Management
12. Bellevue College IT Security Standard: External Data Transfer
13. Bellevue College IT Security Standard: Media Disposal
14. Bellevue College IT Security Standard: Web Servers
15. Bellevue College IT Security Standard: Internet Software Security
16. Bellevue College IT Security Standard: E-Commerce

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