



---

3000 Landerholm Circle SE • Bellevue, WA 98007-6484 • [www.bellevuecollege.edu](http://www.bellevuecollege.edu)

---

## *IT Security Standard:*

# External Data Transfer

### Introduction

This standard defines the specific procedural and configuration steps taken to implement the Bellevue College IT Security Policy for transferring protected data from Bellevue College to any external entity. The standard will be reviewed on an annual basis or when changes are implemented.

### Scope

When this standard refers to “protected” data, it means data and/or information used for any business and/or educational purpose on campus that has been defined by the Bellevue College IT security standard addressing “Data and Information Security” as “*Sensitive*”, “*Confidential*”, and/or “*Information Requiring Special Handling*.”

This standard applies to all protected data and/or information gathered, stored or processed using Bellevue College computing systems and applies to all individuals on campus who handle this data. The standard applies to any transfer of information to an external entity, including the processes and procedures developed by Bellevue College in conjunction with the Center for Information Services (CIS) to transfer data directly from Bellevue College's production processor.

### 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

Bellevue College often shares data with various technology vendors, government agencies, and other entities with which the college has business relationships. Proper protection and handling of this data is of the highest priority, both while in transit and while stored, but technological innovation has put such data more at risk than ever before. Given the sensitive nature of some of the protected data managed at the college, the most significant threats are:

1. Malicious and/or unauthorized disclosure of information
2. Malicious and/or unauthorized modification or deletion of information

Given the nature of the assets being protected and the nature of the threat, the primary risk associated with the administrative applications is with unauthorized access to information, resulting in either disclosure or modification. This would likely be used to commit some type of fraud or theft, but even simple disclosure of protected information is contrary to Bellevue College policy.

## Standard

When transferring protected data outside the college across a public network, or when physically sharing such data using storage media with a business partner who is not a member of the Washington Community Technical Colleges (WCTC) institution, care must be taken to ensure that the integrity and confidentiality of the data is maintained. Precautions to guard protected data must begin as soon as it leaves the server and it must be encrypted any time it is stored by or in transit to a non-Bellevue College entity.

### 1. General

- a. Files being physically shared or transferred through electronic means will likely be downloaded from the server housing the information to a workstation, and then manipulated in some manner.
  - i. Protected data will not be stored on any drive on a shared workstation or server storage space accessible to users not authorized to access the information.
  - ii. Protected data will be deleted from a workstation drive as soon as practical after its immediate use.
  - iii. When not in immediate use, protected data copied from its native location and saved on any storage media—including a workstation hard drive—will be encrypted using an industry standard strong encryption algorithm as defined by the Bellevue College IT security standard addressing “Encryption Tools and Protocols.”
    1. Strong encryption is absolutely *mandatory* for protected data stored for any length of time on a portable storage device of any kind in order to protect the data in the event of the loss or theft of the storage device.
      - a. This includes portable computing system (i.e. laptop or tablet) drives, DVD/CD-ROMs, floppy disks, thumb or flash drives, and/or storage cards.
      - b. More guidelines and information may be found in the Bellevue College IT security standard addressing “Portable Storage Devices.”
    2. Encryption required when protected data is transferred across a public network depends on the type of transfer, and is further described below. Protected data will be secured at all times while in transit.
- b. The guidelines articulated in this standard will apply if in some circumstances the encryption of data being viewed or used during an interactive session with Bellevue College computers is ever required.
- c. If any federal or state regulations require encryption of other Bellevue College data, whether that data is defined by Bellevue College policy or the IT Security Program as “protected” or not, the precautions described in this standard will be followed.
- d. Both endpoints in any electronic exchange of protected data must be assured secure. If unable to get this assurance, a physical transfer of the protected data is preferred.
- e. All transfers of protected electronic data by any means will include a confirmation receipt by the intended recipient of the data. If this confirmation is not built into the sharing mechanism (such as with a secure shell connection) the confirmation must be made independently of the data transfer.

### 2. E-mail Transfers

- a. The most common method of electronic data transfer is through the use of e-mail, usually as attachments. Bellevue College has set up a secure e-mail system to provide communications access to the outside world.
- b. When any protected data is transferred by e-mail from Bellevue College, only Bellevue College-provided campus e-mail will be used. Personal e-mail accounts using service

providers and/or servers outside Bellevue College cannot be assumed to be secure in any manner, and will not be used to transfer protected information.

- c. Protected data transferred via e-mail must be encrypted before sending.
  - i. This applies to any attachments containing protected data as well as e-mail messages themselves.
  - ii. If an e-mail requires encryption, only the tools and protocols authorized through the Bellevue College IT security standard addressing "Encryption Tools and Protocols" may be used.
  - iii. If encryption of e-mail is required, the encryption method and process will be configured so that only the intended recipient of the e-mail can view the data in its original, unencrypted state.
  - iv. Archiving of e-mail generated from Bellevue College's network, encrypted or not, will follow the expectations of the Bellevue College IT security standard addressing "Retention of Electronic Records."
  - v. Bellevue College e-mail servers will be configured to allow unencryption of a message sent by a Bellevue College user by IT support personnel, if needed. Such unencryption by an individual not the original sender of the message requires authorization by the Dean of Information Resources or authorized designee.

### **3. Web-based Transfer**

- a. Web-based transfer is used by some federal agencies for submitting data on an annual basis (i.e., Social Security Administration, Internal Revenue Service, Immigration and Naturalization Services.)
- b. When any protected data from Bellevue College is transferred through the web the data will only be transferred over a Secured Socket Layer (SSL) encrypted link. SSL provides secure communications, authentication of the server, and data integrity of the message packet for transferred data.

### **4. Dial-in Transfers**

- a. Dial-in transfers tend to be a manual process, which is not well-suited for automation. However, at least one federal agency uses this methodology for submitting data on an annual basis (Internal Revenue Service.)
- b. When any data is being transferred from Bellevue College in this manner, the Bellevue College representative is dialing into a private network to transfer the file(s), so there is little inherent risk with the transfer itself. However, appropriate precautions still need to be taken to protect the data.

### **5. Secure Shell (SSH) and File Transfer Protocol (FTP)**

- a. Protected data may be exchanged (sent or received) with business partners via SSH or FTP, if the following criteria are met:
  - i. SSH will be used at all times in preference to FTP. However, it is recognized this may not always be possible.
  - ii. SSH transfers will be compliant with the Bellevue College IT Security Standard addressing "SSH Configuration."
  - iii. Firewall rules will be configured to restrict access to the smallest range of IP addresses (ingress or egress) as possible.
  - iv. Any account passwords required, either internally or those to be used by Bellevue College personnel to log into an external entity's site, will be managed in accordance with the Bellevue College IT security standard addressing "Password Management", recognizing that the external entity also has policies and procedures to be respected.

- v. RSA (Rivest-Shamir-Adleman public-key authentication) may also be used for either outbound or incoming connections. However, this permission does not change the account password management requirements.
- vi. If a null RSA pass-phrase is used, it will be disclosed to the Bellevue College IT Security Administrator. Instances of the use of Null pass-phrases will be reviewed and documented as exceptions to the Bellevue College IT security standard addressing "SSH Configuration."
- vii. FTP data will be encrypted and signed with PGP in accordance with the Bellevue College IT security standard addressing "Encryption Tools and Protocols."

## **6. Additional Technologies**

- a. Other industry standard methods for providing a secure method of transfer may be used when deemed appropriate by the Dean of Information Resources or designee. These include:
  - i. Hypertext Transfer Protocol Secure (HTTPS or S-HTTP)
  - ii. Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - iii. Virtual Private Networks (VPN) which utilize PKI (digital certificate) technology and Internet-based standards for secure network sessions

## **7. Tape, Floppy Disk, or Hard Copy Transfer**

- a. Data may be transferred to business partners via physical media if that is the only option provided by that entity.
- b. The outer case and the media itself will be clearly marked as being property of Bellevue College and that it contains confidential information which must not be further disseminated.
- c. Hard copy reports containing protected data, if used, will have a cover sheet that clearly identifies the report as property of Bellevue College and that it contains confidential information. If possible, each page of the report should contain the same labeling information in a header, footer, or "watermark".
- d. Documentation (preferably contained on the media, but at least provided through a cover letter) accompanying any physical media will provide the recipient with instruction regarding how to dispose of the data and media when they are finished with it. These instructions will comply with the Bellevue College IT security standard addressing "Media Disposal".

## **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. Department of Information Services, "IT Security Guidelines" 402-G2, Feb. 2006

2. Bellevue College Policy #5150, "Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems"
3. Bellevue College Policy #5000, "Acceptable Use of Bellevue College Computers"
4. Bellevue College IT Security Standard: Data and Information Security
5. Bellevue College IT Security Standard: Electronic Mail Configuration
6. Bellevue College IT Security Standard: Encryption Tools and Protocols
7. Bellevue College IT Security Standard: Media Disposal
8. Bellevue College IT Security Standard: Portable Storage Devices
9. Bellevue College IT Security Standard: SSH Configuration
10. CIS IT Security Standard on External Data Transfer

Effective Date: July 2003  
Date Last Modified: July 10, 2009