



---

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

---

## *IT Security Standard:*

# Retention of Electronic Records

### Introduction

This standard defines the specific requirements for implementing the Bellevue College IT Security policy with regards to electronic copies of public records that are required by state law to be retained for a specific period of time. This standard will be reviewed on an annual basis or when changes are implemented.

### Scope

This standard applies to all public records as defined by RCW 40.14.10 which exist in electronic form. Public records that exist only in printed form are not governed in any way by this standard, but electronic records which are converted to hard copy printouts for retention purposes do fall under the scope of this standard. This standard is intended to supplement state law and Bellevue College administrative policies governing the retention, storage, archiving and disposal of records, all of which continue to apply to the procedures and processes described here.

### 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 has a significant responsibility for maintaining records of the services rendered by the college and the business transacted in performing those services. These records are protected by various laws, policies, and standards while being created and actively used. Additionally, state and institutional policies require some of these records to be retained for a specified period of time after they are no longer in active use.

Because many of these archived records may need to be stored in electronic format, it is imperative that established record retention procedures are carefully followed and that campus users maintain vigilant security of data once it is archived. As with data stored and maintained on Bellevue College networks and computers, carefully managing archived records and limiting access only to authorized users is a security priority.

The most significant risks related to creating, storing and accessing retained electronic records are similar to the risks associated with the data in its native state:

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.

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 use of the network itself, loss of revenue, loss of reputation and the potential for litigation. Such disclosure will likely also be a violation of local, state and/or federal law.

## Standard

### **A. Introduction**

1. Washington state law, at RCW Chapter 40.14, requires that all public state records are retained, archived and disposed of appropriately after their active business use is completed in accordance with schedules approved by the State Records Committee. Thus, it is illegal in Washington to destroy an original public record in any form without following established records disposition procedures. Bellevue College policy #6900, "Records Storage and Disposal" and its accompanying Retention Schedules database establish the campus procedures used to archive public college records under the auspices of that state law, and impart the authority for the retention and for the destruction or transfer of such records.
2. Each individual campus unit has responsibility for implementing the procedures described under the Bellevue College policy.

### **B. Electronic Records**

1. The policy makes clear that all Bellevue College "...information systems, including...electronic, shall preserve the integrity and accessibility of the public records they hold for the duration of the established retention periods." This means that documents created through electronic means, such as e-mail, web pages and web-based systems may be retainable public state records, as well. All electronic records that are public records must be identified, scheduled and retained just like records in other formats.
2. Obviously, some records created or stored electronically may be of a transitory nature and have no retention value. Others are used as a means of conducting official business between Bellevue College and its clients, and carry legally mandated retention requirements. Essentially, the content of the electronic record determines whether a document needs archived and how long the archival record will be maintained.
3. Just as they were in their actively-used format, all electronic records retained in compliance with state law, Bellevue College policy or this standard must continue to meet confidentiality requirements, including the Public Records Privacy Protections as spelled out in Executive Order 00-03, and must be protected from disclosure in accordance with the Bellevue College IT security standard addressing "Data and Information Security."
4. **Note:** It would be very difficult and expensive for Bellevue College to duplicate every possible configuration of software and hardware that might at any time have been in use on campus in order to keep retained electronic records accessible. Therefore, it is recommended that archiving of those public records requiring a long-term retention period (3 years or greater) use a non-electronic means, such as producing a paper copy for filing purposes whenever possible to eliminate possible data migration problems.
5. **Electronic mail (e-mail)**
  - a. Electronic mail is primarily a communication system and is not in and of itself subject to retention. However, e-mail messages—the electronic documents created or received using an e-mail system—may contain brief notes, may be formal and substantive documents, and may also have separate documents transmitted with the message as an attachment, all of which need to be appropriately archived.

- b. Proper retention and/or disposition of e-mail messages is always related to the information they contain or the purpose they serve.
- c. For the purpose of satisfying public record laws, e-mail is defined as not only the messages sent and received by e-mail systems, but all transmission and receipt data as well. This includes the content of the message, transactional information, and any attachments associated with the message—all of which are considered a part of the retainable record.
- d. Determining which individual or unit maintains the primary record copy of a message (defined as the *original* message that must be retained according to the retention schedule) is vital to e-mail management. Generally speaking, the individual who sends an e-mail message should maintain the record copy of the message.
- e. The proper length of retention for messages and attachments sent or received electronically is based on considering each message just as if it was conveyed on paper, and must be managed individually according to the approved retention schedule for the information contained within them.
  - i. Messages which contain public records must be identified, managed, protected, and retained as long as needed for ongoing operations, audits, legal proceedings, research, or any other known purpose.
  - ii. Messages created or received in the transaction of public business and retained as evidence of official policies, actions, decisions or transactions are also retainable public records.
  - iii. Messages that have other valuable informational content relating to state business are also considered a public record.
- f. E-mail messages should be indexed in an organized and consistent pattern reflecting the manner in which the records are used and referenced. Messages should be stored in a filing system that is logical and searchable.
- g. Samples types of e-mail content that are usually public records, which must meet records retention requirements before being destroyed, are listed below; this list is not comprehensive:
  - i. Policy and Procedure Directives
  - ii. Correspondence or memoranda related to official Bellevue College business
  - iii. Agenda and minutes of meetings
  - iv. Documents related to legal or audit issues
  - v. Messages which document Bellevue College actions, decisions, operations and responsibilities
  - vi. Documents that initiate, authorize or complete a business transaction
  - vii. Drafts of documents that are circulated for comment or approval
  - viii. Final reports or recommendations
  - ix. Executive appointment calendars
  - x. E-Mail distribution lists
  - xi. Routine information requests
- h. An e-mail message that is considered to have no administrative, legal, fiscal or archival requirements for its retention should be deleted as soon as it has served its purpose. Types of content sent via e-mail which typically have no retention value and may be destroyed when no longer needed include:
  - i. Personal messages and announcements not related to official business (though these types of e-mail may contain evidence or historical material, which then should be retained)
  - ii. Information-only copies or extracts of document distributed for convenience of reference

- iii. Published reference materials
  - iv. Uncirculated preliminary drafts of documents
  - v. Copies of inter- or intra-agency memoranda, bulletins or directions of a general information and non-continuing nature.
  - vi. Announcements of social events, such as retirement parties or celebrations.
- i. To assure appropriate retention of public records generated or received through the e-mail system, e-mail and attachments should be retained in e-mail format only as long as they are being worked on or distributed. When archived, they should be transferred to paper, disk, or to a network storage location and maintained according to the retention period required for the informational content of each message.
- i. When e-mail messages are converted to print for archival purposes, the printed version must include the name of the sender, the name of the recipient, and the date and time of the transmission and/or receipt.

## 6. Web sites

- a. Bellevue College has a responsibility to the citizens of the state of Washington to capture, maintain, and properly dispose of all public records generated by the college. Because some college web sites contain and generate public records as defined by law, archives of web sites must often be maintained. Obviously, a relatively static web site comprised of simple documents with low interactivity will have different requirements for maintenance than complex web-based documents or a highly interactive web site.
- b. Archived records of web sites must be able to meet any legal obligations, and must be able to provide evidence of present and past positions, advice, guidance, transactions or instruction on any particular matter.
- c. Records which document the processes involved in planning, designing, producing and maintaining web resources should also be captured and retained appropriately. This includes documentation of any changes to web sites, which need to be tracked and recorded.
- d. Some web sites used as a means of conducting official business may already capture and retain individual records into a separate, established record-keeping system, and do not need to be archived simply because they are on a web site. However:
  - i. Content that is created for placement directly on web sites which contains information or public records which are required to be retained must be archived, including sufficient data documenting the content, context and structure of the records and their placement on the web site.
- e. The retained electronic records of public web sites must be authentic, reliable, accurate, and provide durable evidence of web-based activity. Units maintaining captured web-based records over time should develop archival procedures which:
  - i. Ensure that records are stored in widely accepted, technology-neutral storage and data interchange formats, such as XHTML.
  - ii. Maintain master archive sets at different locations and in different formats, if necessary.
  - iii. Perform periodic random spot checks to monitor functionality and integrity of the retained records.
  - iv. Refresh the retained media if technology changes. Any loss of functionality, content or appearance that occurs as a result of reformatting or data migration should be fully documented.
- f. Full backups of web sites on appropriate storable media may be used to create archival copies of web content.
- g. Web site records also document both the structure and the public face of Bellevue College and—thus having historical value—may need to be transferred to the State Archives at the end of their retention period.

## **C. Responsibilities**

### **1. Campus Units**

- a. Unit supervisors and individual employees must work with the college Records Officer to inventory and include e-mail records and web content when meeting retention schedules. As needed, units will develop their own procedures for meeting these requirements, but must also comply with the following:
- b. Each campus unit must individually identify those classes of e-mail messages for which it has primary retention responsibilities and which must be appropriately retained as records of the unit's specific official and/or public activities.
  - i. If another state agency or Bellevue College office has the primary responsibility for keeping the record copy of an electronic document and a unit has no business need to retain it, any copy of the document within the unit is considered an informational copy and is subject to deletion/destruction at will.
- c. Decisions regarding which individual web sites must be retained need to be made by the campus unit responsible for the site, and must be based on the content of the particular web site. Units generating public records with or through web sites should inventory these sites and include electronic records of them when conforming with their records retention schedule.
- d. Units will ensure that retained information remains accessible for the entire retention period of the record series.
  - i. Individual units must take into account the security and retrieval requirements of both the current and the future users of the records when establishing archival methods. These users may include unit personnel, researchers and the public.
  - ii. Units must ensure proper environmental conditions for stored records and will employ periodic recopying as needed.
  - iii. Units will develop and use appropriate strategies to preserve data by migration from one generation of technology to another when required.
    - If data is not migrated, access to the records requires preserving the data, the storage medium in which the data is kept, and whatever hardware, operating system, and software applications are needed to view and use the data until the retention period has been met.
  - iv. When storing electronic media containing archival materials, campus units should observe the published state "Environmental Standards or Best Practices for Storage of Electronic Media", ensuring :
    - Temperature ranges meet standards and best practices recommended for the media stored.
    - Humidity ranges meet standards or best practices recommended for the media stored.
    - Media is stored in a closed container to protect from dust and fingerprints.
    - Magnetic tape, if used, should be rewound.
- e. Access to stored or retained data needs to be limited to only those authorized to access the data in its native state.
- f. Individuals must regularly transfer public records to an organized, secure and accessible filing system. Retained electronic records must be stored in a manner which protects them from subsequent alteration. E-mail messages must be protected from inadvertent loss or destruction through compliance with backup requirements and procedures.

### **2. Information Resources**

- a. Information Resources has a dual role in the retention of electronic records. First of all, IR is a campus unit like any other and must meet the requirements for records retention of their own records just as any other campus unit. In addition, IR has the responsibility

of assisting campus users in the retention of their unit electronic records and in helping to preserve the means to access any stored electronic records during their retention period.

- b. Information Resources will advise and assist the college Records Officer and campus units regarding any technical aspects of retaining electronic records.
- c. IR will consult in evaluating the value of various types of records at the request of campus units, if needed.
- d. While Information Resources creates backups of both web sites and e-mail as a part of normal disaster recovery strategies, such back-ups are regularly overwritten and are not useful for records retention purposes.

#### **D. State Archives**

1. This standard does not govern any actions by the State Archives. The below is included as advisory information for Bellevue College campus users. Additional information may be found at the State Archives web site at <http://www.secstate.wa.gov/archives>.
  - a. The State Archives can perform consultation services in document imaging, conversion of digital, paper or microform documents to other formats, and records destruction.
  - b. Units should coordinate all activities involving the State Archives through the campus Records Officer.

### **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. Chapter 40.14 RCW, "Preservation and Destruction of Public Records"
2. Bellevue College Policy #6900, "Records Storage and Disposal"
3. General Records Retention Schedules, Office of the Secretary of State and the Division of Archives and Records, Summer, 2001
4. Governor's Executive Order 00-03, "Public Records Privacy Protections"
5. Guidelines for Developing Policy and Establishing Procedures for E-mail, Office of the Secretary of State, March, 2001
6. Bellevue College IT Security Standard: Data and Information Security

Effective Date:	May 2006
Date Last Modified:	July 10, 2009