



IT Security Standard:

Data and Program Backup

Introduction

This standard defines the steps needed to implement Bellevue College policy # 5250: Information Technology (IT) Security regarding the backup of data and program files. This standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard describes the specific Bellevue College IT security program expectations for the handling of the backup and recovery of data and/or program files on campus. This standard conforms to the expectations of the Washington state Information Services Board (ISB) IT security guidelines as well as the Washington state Department of Information Services (DIS) IT Information Technology Disaster Recovery and Business Resumption Planning Guidelines with regard to data security and recovery.

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

The technology used at Bellevue College to support the college's educational, business and administrative missions is dynamic, volatile and very critical to daily operations of Bellevue College. These functions would be severely impacted by the loss of computing data or program files. Without clearly communicated backup protocols significant disruption of services and loss of information can occur in the event of power or equipment failures.

The most significant threats necessitating the use of backups are:

1. Malicious, unauthorized or accidental modification to Bellevue College systems and networks
2. Malicious, unauthorized or accidental modification to Bellevue College data
3. Compromise or loss of protected, sensitive data
4. Loss of services or equipment and software functionality

Given the nature of the technology assets and the nature of the threat, the main risks associated with a lack of a dynamic backup program are the permanent loss of vital, sensitive, unique or irreplaceable data. All of these threats have associated risks of loss of revenue, dissatisfaction of those to whom Bellevue College provides services, interruption of productive work, and a loss of reputation.

Standard

A. Introduction

1. Backups in the Information Technology environment are generally assumed to be copies of files and programs stored on magnetic media. However, it may be preferable to backup and store some information in hard copy form, such as printouts or microfiche. For the purposes of this standard, the term “backup” will be defined as including both electronic and printed copies of files and data.
2. In all cases, electronic backup media must be stored in such a way as to assure both its magnetic integrity and its physical security. Backups in non-electronic form require the same physical security considerations as do electronic media.
3. Any form of backup must be handled and stored in accordance with appropriate Bellevue College privacy policies and standards governing the contents of the data included in the backup, including the Bellevue College IT security standards addressing “Data and Information Security” and “Database Management”, and must be disposed of in accordance with the Bellevue College IT security standard addressing “Media Disposal.”

B. Individual Workstations

1. Bellevue College technical support personnel do not routinely backup individual workstations. The Bellevue College Help Desk can provide assistance with creating an individual backup plan, but Bellevue College staff are expected to appropriately create and store important files on the backup media of their choice.
 - a. There is no requirement to backup any program files on individual workstations; these will be reinstalled in the event of a program failure.
 - b. To support individuals in properly preserving their vital data, Bellevue College may purchase site licenses for backup software.
 - c. Bellevue College IT support personnel will assist users in restoring any data from backup, if such restoration is necessary. This may include entire system restorations from support master disks, or assistance to users in restoring from their individual backups.
 - d. Individuals authorized to use personal equipment at Bellevue College, such as computers and hand-held devices, are personally responsible for backup and restoration of any system or data files necessary to ensure the uninterrupted functioning of those resources.
 - i. In accordance with the Bellevue College IT security standard addressing “Connecting Non-Bellevue College Equipment to the Bellevue College Network”, if non-Bellevue College equipment needs restoration, Bellevue College technical support personnel will only provide information; they will not support or configure any non-college equipment.
2. All campus web page maintainers are responsible for keeping backup copies of the pages for which they are responsible, as required by the Bellevue College IT security standard addressing “Web Space Usage” and by Bellevue College policy #5200: “Student Network Web Space Usage.”

C. Server, Network and Administrative System Responsibilities

1. Backups of server and administrative systems under the responsibility of IR personnel or authorized designees will be made, handled and stored in accordance with various Bellevue College IT security standards, including:
 - a. Data and Information Security
 - b. Data Management
 - c. Firewall Configuration and Change Management
 - d. MPE System Configuration
 - e. Network Device Configuration
 - f. Password Management
 - g. Phone System Configuration
 - h. Physical Security
 - i. Security Privileges
 - j. SSH Configuration
 - k. Video and Television Services

2. IR personnel will regularly backup and archive files and programs stored on any network data storage space or server, in anticipation of potential system-wide disaster recovery requirements. Further information regarding off-site storage and other related responsibilities are articulated in the Bellevue College "Disaster Recovery and Business Continuity Plan," which is maintained by IR under the requirements of the Bellevue College IT security standard addressing "Disaster Recovery."
3. IR personnel will conduct periodic tests to restore Bellevue College data from backup media, following procedures supportive of the processes described in the Bellevue College "Disaster Recovery and Business Continuity Plan."

D. Network Data Storage

1. In accordance with the Bellevue College IT security standard providing campus users access to "Network Data Storage", individual work files stored on the network data storage space will be regularly archived by IR in anticipation of potential system-wide disaster recovery.
 - a. Although IR will make a good faith effort to recover lost or accidentally deleted files, this is a less-than-adequate means of backup for individual data. Therefore, individual users are responsible for developing their own contingency data backup procedures for data stored on any Bellevue College network.

E. Temporary Backups

1. Technical support personnel may make and keep backups of individual computing systems prior to troubleshooting, making any configuration changes, or in response to investigations conducted under the Bellevue College IT security standard addressing "Intrusion Detection and Incident Response".
 - a. Temporary backups will be erased once the purpose of the backup has been completed, and
 - b. Temporary backups will not be stored longer than one (1) month without the approval of the Dean of Information Resources, or an authorized designee.

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. Bellevue College Policy #5200: Student Network Web Space Usage
2. Bellevue College Policy #5250: Information Technology (IT) Security
3. Bellevue College Disaster Recovery and Business Continuity Plan
4. Bellevue College IT Security Standard: Database Management
5. Bellevue College IT Security Standard: Data and Information Security
6. Bellevue College IT Security Standard: Disaster Recovery
7. Bellevue College IT Security Standard: Intrusion Detection and Incident Response
8. Bellevue College IT Security Standard: Media Disposal
9. Bellevue College IT Security Standard: Network Data Storage

10. Bellevue College IT Security Standard: *Network Device Configuration*
11. Bellevue College IT Security Standard: *Connecting Non-Bellevue College Equipment to the Bellevue College Network*
12. Bellevue College IT Security Standard: *Web Space Usage*
13. Bellevue College IT Security Standard: *Firewall Configuration and Change Management*
14. Bellevue College IT Security Standard: *MPE System Configuration*
15. Bellevue College IT Security Standard: *Password Management*
16. Bellevue College IT Security Standard: *Phone System Configuration*
17. Bellevue College IT Security Standard: *Physical Security*
18. Bellevue College IT Security Standard: *Security Privileges*
19. Bellevue College IT Security Standard: *SSH Configuration*
20. Bellevue College IT Security Standard: *Video and Television Services*
21. DIS, *IT Disaster Recovery and Business Resumption Planning Guidelines*, <http://isb.wa.gov/policies/portfolio/502G.doc>, April, 2002
22. DIS, *IT Security Guidelines*, <http://isb.wa.gov/policies/portfolio/402G.doc>, February, 2006

Effective Date: July 2003
Date Last Modified: April 12, 2009