



3000 Landerholm Circle SE • Bellevue, WA 98007-6484 • www.bellevuecollege.edu

IT Security Standard:

Network Data Storage

Introduction

This standard defines the steps needed to implement the Bellevue College IT Security Policy with regard to Bellevue College technology users storing data on network storage devices. This standard will be reviewed on an annual basis or when changes are implemented.

Scope

This document defines the standards and expectations related to the use of network storage for data by Bellevue College technology users. This includes employees, non-employees authorized to use Bellevue College networks and technology resources, and students. The servers and data storage resources covered under this standard may be accessed either through the Administrative Network and/or the Academic Network.

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

Providing network-based data storage resources to computer users on the Bellevue College networks creates slightly higher risks to the computer-based assets at Bellevue College than already exist for these users. By creating additional paths of access to the Bellevue College networks, additional vulnerabilities and paths for unauthorized access are created as well.

Because of the higher level of access inherent in providing network data storage to users, and the great dependence on computing technology at Bellevue College, the associated risks are similar to those addressed in the Bellevue College IT security standards addressing "Password Management" and "Security Privileges." The most significant of which are:

1. Malicious and/or unauthorized access to systems, data and/or services
2. Maliciously increasing privileges to include unauthorized systems
3. Theft, fraudulent use, and/or malicious destruction, manipulation and/or disclosure of critical data and/or services
4. Accidental destruction of data
5. Malicious and/or unauthorized access to controlling components (e.g., routers, DNS, domain controllers)
6. Accidental and/or malicious interruptions to the Bellevue College operating environment

Given the nature of the asset and the nature of the threat, all risks associated with granting users network data storage access are significant, and could represent great loss to Bellevue College.

Standard

Traditionally, most computer users at Bellevue College have stored their computer data either on the hard drives of the computers they use, or on removable media such as floppy and Zip disks. This method works well for local and for temporary storage needs as well as for storage of size-limited data. However, these methods do not address the problem of consistent data access away from the user's local workstation, nor are they flexible enough for the educational and business needs of many Bellevue College users.

Information Resources (IR) will provide data storage locations which will allow employees and students to store and access critical data in secure and protected network directories accessible from any computer authorized and able to connect to the Bellevue College networks. These data storage locations will be password-secured and tied to personal user account names.

Individuals may request and be granted access to this network data storage space if such capacity is necessary to effectively and professionally complete assigned responsibilities.

General

The following requirements apply to all users being granted network data storage under the provisions and procedures in this standard:

1. Network data storage is intended for critical data access from multiple locations; it is not intended to archive large amounts of non-critical or personal data.
2. All storage limits will be strictly enforced. Users who exceed their storage limitations will receive an automated caution, and will lose the ability to save additional data in their network directories.
3. Information Resources reserves the right to suspend any individual's network data storage access if illegal data or data that is prohibited by any Bellevue College policy is stored in these locations. Storage of copyrighted materials outside of individual ownership or academic fair use is prohibited.
4. Network data storage will not be used to install or run executable software applications under any circumstances, or to circumvent any provisions of the Bellevue College Software Licensing Compliance Policy. Such use will result in immediate termination of network data storage privileges.
5. Data storage space will be regularly archived by IR in anticipation of potential system-wide disaster recovery. However, though IR will make a good faith effort to recover lost or accidentally deleted files, individual users are responsible for developing their own contingency data backup procedures.
6. The Bellevue College IT Security Administrator, or authorized designee, will file and maintain all completed and approved Request for Network Data Storage forms.

Faculty and Staff

1. Individuals desiring access to network data storage will make a formal request using the Request for Network Data Storage Form. Access to network data storage will only be granted upon approval by the Bellevue College IT Security Administrator and/or the Dean of Information Resources.
2. Once network data storage space has been granted, the requesting individual will be notified by e-mail on how to access the resource.
3. Data storage locations for faculty and staff will be servers accessed through the Administrative Network, unless there is an exception based on a specific educational purpose and/or academic necessity for it to be located on the Academic server.
4. Members of Bellevue College faculty and staff approved to have network data storage space will be given access to 300 MB of network data storage.

5. In the event that extraordinary circumstances require a faculty or staff member to have increased storage in order to perform professional responsibilities, a request for additional space will be made to the Bellevue College IT Security Administrator and/or the Dean of Information Resources, or authorized designee, using the Request for Network Data Storage Form.

Non-Bellevue College Employees

1. Individuals desiring access to network data storage will make a formal request using the Request for Network Data Storage Form. Access to network data storage will only be granted upon approval by the Bellevue College IT Security Administrator and/or the Dean of Information Resources, or authorized designee, and will be approved by the Bellevue College administrator to whom the individual reports.
2. Once network data storage space has been granted, the requesting individual will be notified by e-mail on how to access the resource.
3. The individual must have previously been granted access to the Bellevue College networks under the authority of the Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems Policy, and have a valid login name and password to be allowed access to network data storage.
4. The storage space must be required for the individual to be able to perform official Bellevue College duties. The amount of space granted will be contingent upon the business and/or educational need which precipitated the specific request.
5. Data storage for non-Bellevue College employees will be located on servers accessed through the Administrative Network, unless there is an exception based on a specific educational purpose and/or academic necessity for it to be located on the Academic server.

Students

1. Students will be automatically granted access to 100 MB of network data storage space upon creation of their Academic Network login accounts following the procedures described in the Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems Policy.
2. Access to network data storage space will be contingent upon the student being registered for the current quarter.
3. Data storage locations for students will be located on servers accessed through the Academic Network.
4. In the event more storage is required in order to meet educational demands, a request for additional space will need to be approved by the Bellevue College IT Security Administrator and/or the Dean of Information Resources.
5. Student data will *not* be archived and all student users will develop individual contingency data backup procedures.
6. The contents of all student data directories will be deleted one week after the conclusion of Summer quarter each year.

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. Bellevue College Acceptable Use of State Resources Policy
2. Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems Policy
3. Acceptable Use of Bellevue College Computers Policy
4. Bellevue College Copyright and The Right of Fair Use Policy
5. Bellevue College Software Licensing Compliance Policy
6. Bellevue College IT Security Standard: Software Management
7. Bellevue College IT Security Standard: Password Management
8. Bellevue College IT Security Standard: Security Privileges

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