



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

IT Security Standard:

User Management

Introduction

This standard defines the expectations of the Bellevue College Information Technology (IT) Policy with respect to the management and documentation of access to technology by campus users. This standard will help assure the integrity and reliability of the Bellevue College internal networks, the computers on those networks, and the software installed on those computers. This standard will be reviewed on an annual basis or when changes are implemented.

Scope

The processes and procedures identified in this standard apply to all users accessing or wanting to access any Bellevue College technologies. The recommendations and procedures identified in this standard are not intended to supersede Bellevue College Human Resources procedures and policies, but to support the implementation of those requirements with regard to the use of technology resources.

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

One of the key security links in any technology system is the users of the technology. Users are deliberately granted rights to use protected institutional resources that are otherwise hardened against unauthorized access, and are trusted not to abuse that right of entry. If a user is given privileges to a system and is ignorant of or chooses to disregard good security practices, the results can be the same as not having security deployed in the first place.

Given the inherent security risks in mis-managing users and the privileges granted to them, the threats to Bellevue College systems include:

1. Unauthorized access to sensitive or confidential data – malicious or accidental
2. Unauthorized modification of data – malicious
3. Theft of services – malicious
4. Damage to or loss of equipment or resources – malicious

In analyzing the nature of the threat to Bellevue College resources associated with misuse or misapplication of user privileges and access, the primary risk is unauthorized access to resources and an associated risk of allowing malicious access through inactive or no longer authorized accounts. These

risks may subject the institution to other risks, such as disclosure of protected information, interruption or denial of services, and a loss of reputation.

Secondary to these threats is the potential for inappropriate use of the resources, including violations of state and/or federal law and policies, excessive bandwidth use, uses inconsistent with the Bellevue College mission, or uses that are in violation of the Bellevue College Acceptable Use policies.

Standard

While the technology used to support the educational, business and administrative missions of Bellevue Community College is reasonably secured by a robust IT security program, the complexity and variety of the technologies deployed across campus create a system with inherent risk.

Because misappropriation or misuse of a user's access is potentially one of the greatest threats to the continued availability of these resources, deliberately managing appropriate access to computers and the network with carefully considered procedures for granting, managing and withdrawing privileges over the life of a user's association with the college must be in place to protect all vital college resources.

New Users

New users of Bellevue College technology resources must be assisted in establishing their access and rights to the systems they will use while working for the college and in initial communications with IR.

All individuals using Bellevue College network or computing resources are required to have log-in accounts. The specific procedures for establishing network accounts for various classes of users are different from one another, and are established in Bellevue College policy #5150, "Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems":

1. **Employees and Non-Employee**

Accounts for new employees and for non-employees who require access to Bellevue College networks and/or systems are governed under the section of Bellevue College policy #5150 entitled "*Employee and Non-Employee Permission for Network Use.*" Approval for an account rests with an appropriate Bellevue College administrator; establishment of the accounts is accomplished by Information Resources technical support personnel.

Primary responsibility for assisting new employees through the process and for communicating with IR rests with their hiring authority supervisor. For all non-employees, these responsibilities rest with their Bellevue College contact person.

2. **Students**

Network log-in accounts for students are regulated under the section of Bellevue College policy #5150 entitled "*Student Permission for Network Use.*" Responsibility for assisting students in establishing access to appropriate systems rests directly with IR, through its web-based resources, including the Student Technology Support Center.

A network account does not grant permission to the administrative HP data systems. The requirements for establishing credentials to access those additional resources are articulated in the Bellevue College IT security standard addressing "HP Administrative System Access."

Changing User Information

Periodically, because individual's names may change for a variety of reasons, changes need to be made to network user credentials. All requests for changes to network account information must be submitted to Request Center and will be coordinated with Human Resources (HR) records.

Because of the technical and security restrictions in place, user credentials for the HP Administrative systems will not be changed once they have been established.

1. **Network name changes**

- a. Employees

- i. Prior to requesting an account name change, the requestor must communicate with HR to ensure the official employee record reflects the appropriate name.

- ii. IR support personnel will follow-up with the individual requesting a name change and with HR to ensure any requested account name change is appropriate and in harmony with HR records prior to making any account name change.
 - b. Non-employees and Students
 - i. Account names for non-employees and/or students will not be changed.
- 2. **Student ID/Staff ID (SID)/Employee ID (EID) changes**

When SID or EID numbers have been changed, IR will modify all appropriate account records to reflect the change after being notified of the change. Note: for brevity and the purposes of this standard, SID will be used from here on to refer to both SID and/or EID numbers.

 - a. Employees
 - i. All employee SID changes must be requested through HR.
 - ii. HR and IR will jointly develop a process for making notifications to IR regarding any SID change affecting an employee.
 - b. Students
 - i. Student SIDs are managed through Student Services and all requests for changes must be submitted to that office.
 - ii. Student Services and IR will jointly develop a process for making notifications to IR regarding changes to student SIDs.
 - c. Non-Employees
 - i. Non-employee network users do not have SID assigned.

Password changes

It is not uncommon for campus users to need assistance in changing or resetting their network passwords. Password changes are managed through the Help Desk, but specific security procedures must be followed to appropriately change an individual's password.

In accordance with Bellevue College policy #5150, "Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems", account passwords for new users may be given to the individual employee, to his/her immediate supervisor, or to an individual identified on the request form as the unit contact person. However, disseminating information regarding *changed* passwords is more strictly governed.

1. **Employees**

Employees may change their own passwords through a number of campus resources:

- a. The best method of changing a password is through the *MyBC* portal, which contains a Password Management Tool, linked to the portal splash page as an "eTool". The site is also directly accessible at <http://www.bcc.ctc.edu/password>.
- b. As a secondary method of changing a password employees may request a temporary change to their password through the Help Desk, either in person or by phone.
 - i. Individuals are required to provide positive confirmation of their identity when requesting a password change.
 - 1. This may be done in person by providing photo identification.
 - 2. Requests over the phone for password changes require alternate confirmation:
 - a. Requestors must provide to the Help Desk support person their first and last name, their SID, and their date of birth.
 - i. If the employee does not know her/his SID, they must contact Human Resources or their division secretary for assistance in obtaining that information. No password changes will be made without this information.
 - b. This information from the requestor will be compared to the information available to support personnel through the Employee Verification tool.

- c. If the employee cannot be verified or if their employment status is anything but “Active”, the password will not be changed.
 - ii. Once positive confirmation of identity has been established, Help Desk support personnel may assign a new, temporary password to the individual’s account.
 - 1. Support personnel will notify the requesting individual of the temporary password.
 - 2. The individual will be required to change this temporary password at first log-in.
 - 3. It is recommended that this initial log-in be done using a campus computer.
 - c. Employees may not request a password change on behalf of another employee.
 - d. Supervisors may request a password change on behalf of a subordinate employee, but the new password on another individual’s account will not be given to a supervisor without the specific permission of the Vice-President of Human Resources.
- 2. **Non-Employees**
 Because non-employees do not have the appropriate identifying information available within Bellevue College systems for identity verification, authorized non-employee network users needing their password changed must ask to have it changed in one of two ways:
 - a. In person at the Help Desk.
 - i. Help Desk personnel will confirm the individual’s identity with photo identification before resetting any password.
 - b. The non-employee’s supervisor or Bellevue College contact person may request a password change on behalf of the individual, either through Request Center or the Help Desk.
 - ii. The supervisor and/or contact person may be given the temporary password to pass on to the affected non-employee.
- 3. **Students**
 Students can self-manage their account passwords, including resetting and changing their password, through the Student Account Management web site (<https://www.bcc.ctc.edu/sam>).

Transferring Users

At times, campus technology users are transferred from job-to-job on the campus. Usually this involves a physical move and it often includes a change in the nature of the user’s work on campus. This can include a change in classification or responsibilities, and may affect access to specific network resources, applications and/or files. The procedures listed in #1 and #2 below apply only to cooperative employee users being transferred.

- 1. **Originating Unit**
 If the user’s old unit does not notify IR in a timely manner to make needed changes, the individual may continue to have access to materials and resources inappropriate for their new position.
 - a. When an employee leaves a campus unit and will be assigned to a different campus unit, the individual’s supervisor must notify IR immediately of the change. This notification will be done through Request Center, and should include a request for withdrawal of any privileges to unit network or computing resources that are no longer needed by that individual, such as:
 - i. Installed software applications,
 - ii. Distribution or security lists,
 - iii. Network storage locations,
 - iv. Shared e-mail accounts,
 - v. Specific phones or phone numbers, and/or
 - vi. Specific unit computers,

- vii. Web server account.
 - b. The originating unit supervisor *may not* request a change in the active account of an individual who is continuing employment with the college without HR permission.
 - c. If technical assistance is needed to archive user materials or to transfer unit files from the user to another individual, those needs will be articulated in the Request Center task.
 - d. The Request Center task should also identify if the transferring individual needs electronic data files transferred to the new work location.
 - e. Any transfer of software applications or computing hardware from the originating unit to the new unit pursuant to and coinciding with the transfer of a user will be governed by the “*Transfer and Disposal of Computers and Software*” section of the Bellevue College IT security standard addressing “Software Management.”
2. **New Unit**
- a. The new campus unit must notify IR through Request Center that an existing Bellevue College employee is now assigned to a different unit and supervisor, and must request any needed access to computing or network resources now required for that individual. This may include access to:
 - i. Installed software applications,
 - ii. Any new applications needed,
 - iii. Unit distribution or security groups,
 - iv. Unit network storage locations,
 - v. Shared e-mail accounts,
 - vi. Specific phones or phone numbers, and/or
 - vii. Specific unit computers.
 - b. If the transfer of an individual within the campus includes a change in classification (classified, exempt, faculty) the new unit must identify that change in the Request Center task so the individual may be added to appropriate campus-wide distribution lists.
3. **Other Types of Transferring Users**
- With regard to other classes of campus technology users:
- a. Supervisors will request any technology changes related to transfers of uncooperative employee users through HR, and all IR responses and actions will be at the specific request and direction of the Vice President of HR.
 - b. Non-employee users provide specific services for a specific unit and are not “transferred.”
 - c. Student users are not “transferred” because they are not associated with a campus unit unless employed by that unit. In that case, they would be considered employees.

Employee and Non-Employee User Separation/ Termination

1. **Supervisor Responsibilities**
- a. In addition to responsibilities for notifying HR of the end of an individual’s association with the college, a supervisor will also notify IR of the separation/ termination of anyone with access to campus technology resources. This notification will be made through Request Center, and will:
 - i. Identify the date when the user’s account and access to any technology resources should be rescinded.
 - 1. This may include access to:
 - a. Installed software applications,
 - b. Any shared resources, including:
 - i. Shared e-mail accounts
 - ii. Unit network storage locations
 - iii. Unit distribution or security groups,

- c. Phones,
 - d. Unit computers, including the one assigned to the individual or any other for which privileges have been granted,
 - e. Any campus web sites the individual may have had permission to edit or to manage.
- ii. Identify any Bellevue College technology hardware resources in the possession of the individual and the supervisor's plan for recovery of those assets.
 - iii. Clarify any other special technology requirements associated with the user's separation. This may include, if applicable, requests to:
 - 1. Access or electronically store as an archive any user profile and data files related to the separating employee.
 - a. Both the initial archiving of such information and subsequent access to or deletion of archived information at the supervisor's request must be approved by HR.
 - 2. Change passwords for any affected shared resources.
- b. Supervisors should also communicate with IR regarding requests for redeployment to other unit users of Bellevue College technology resources, especially computers and phones, previously assigned to the separating user.
2. **Information Resources Responsibilities**

After notification, IR will:

- a. Disable separating user access to Bellevue College networks, systems and technology resources.
- b. Replace the hard drive in a computer assigned to a separating individual with a generic Bellevue College drive so the computer may be available for the next user.
- c. Assist the separating individual's unit and HR in storing approved archival data.
- d. Notify the separating individual's unit if it is determined that the individual is the last user to have access to a unit resource, such as a shared department e-mail address, department website, department network space and/or public folder, if applicable.
- e. Make appropriate changes to and/or reassignments of Bellevue College systems and resources, as requested by the supervisor and as approved by HR, if applicable.

Student Separation

Information Resources has responsibility for managing student access to systems. Published IR procedures will govern termination and/or continued student access to Bellevue College resources.

Portal Class Sites

Network accounts associated with instructors who are still pending formally-approved access to Bellevue College technology resources may be created within the active directory for the specific purpose of allowing the automated creation of shared instructional class sites within the Bellevue College SharePoint portal.

1. These "pending authorization" accounts will be used only for this purpose, and will be created by IR with all user privileges to any other Bellevue College resources disabled.
2. "Pending" accounts will be created with a standard user name and a highly secure password, neither of which will be disseminated.
3. Identifying information required by the portal site creation application may be added to the account, if needed.
4. Neither e-mail nor any external accounts will be associated with the account.
5. The account will not be added to any Bellevue College distribution or security groups.

Once formal administrative approval of a previously "pending" account has been received, standard account privileges will be enabled, e-mail will be associated with the account (if requested), and the

password will be reset to college standards. The account name and password will then be provided to the appropriate division contact, who will disseminate it to the faculty member as a new user account.

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 Policy #5000: Acceptable Use of Bellevue College Computers
2. Bellevue College Policy #5100: Software Licensing Compliance
3. Bellevue College Policy #5150: Acceptable Use of the Bellevue College Network and Bellevue College Data Management Systems
4. Bellevue College Policy #5250: Information Technology (IT) Security
5. Bellevue College IT Security Standard: Non-Employee Access to Systems
6. Bellevue College IT Security Standard: Physical Security
7. Bellevue College IT Security Standard: Software Management

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