



IT Security Standard:

Password Management Exceptions

Introduction

This document defines the identified specific exceptions to Bellevue College policy # 5250: Information Technology (IT) Security related to the Bellevue College IT security standard addressing “Password Management.” These exceptions will be reviewed on an annual basis or when changes are implemented, and will be maintained by the Bellevue College IT Security Administrator and/or the Dean of Information Resources.

Scope

This document exercises the exemption granted in the Department of Information Services (DIS) Information Technology (IT) Security Policy for Institutions of Higher Education, pursuant to RCW 43.105.200 and fulfills the requirement within the Bellevue College IT security standard addressing “Password Management” for documentation of the exceptions to the standard. Any deviations from the standard for either business necessity or platform implementation constraints will be appropriately established within this document.

Exceptions

A. Student Computing Exception

1. The creation of student user accounts for the use on Bellevue College’s Student network and computing systems is not required to follow the procedures for requesting and creating accounts as enumerated in the standard.
 - a. The procedure for creation of student accounts will be at the discretion of the system administrators assigned to the Network Server Group (NSG), with the approval of the Dean of Information Resources or authorized designee. Currently, students may create their own accounts via Web access.
 - b. Information Resources will take all due care to ensure that only authorized, registered students are allowed to create user accounts for the Student network.
 - c. Student accounts will not have sufficient privileges to access the administrative networking domain or administrative computers. Security measures will be put into place on the Student network to ensure this is maintained.
 - d. If a student is required to access administrative computing resources for any reason (i.e., part-time employment, internships), the procedure for requesting and creating accounts described in the Bellevue College IT security standard addressing “Password Management” will be followed.
 - e. Student users will be notified of, and acknowledge understanding of, the applicable sections of the standard and of this exception prior to an account being authorized. This notification will be in electronic format.
2. Student user passwords will not be expected to comply with the “*Aging*” section of the “Password Management” standard, but will instead be set to expire at the end of each academic year.
3. Student users will be expected to comply with the “*Password Security*” and “*Remedies*” sections of the “Password Management” standard.

4. Student users will be encouraged to comply with the “*Password Selection*” section of the “*Password Management*” standard, but will not be required to do so.
 - a. The NSG enforces those elements of that section of the standard and sets checks into place to ensure student accounts comply with the spirit of the section, but may lessen the specific requirements to simplify the on-line password creation process.
 - b. Students will be notified of the standard and encouraged to comply with it.
 - c. This lesser level of security for this specific section is allowable because of the lack of business mission critical systems on the Student Network.
5. If an individual is not registered for the subsequent quarter, student user access to the Bellevue College computers, networks and to student e-mail will be disabled at the end of the last day of the quarter for which they were registered. Student accounts and passwords can continue to be used to access the *MyBC* portal

B. Single Login Exception

1. Password controlled logins to the Bellevue College network will be limited to one logon at a time, except in the following circumstances:
 - a. Authorized IT support personnel, such as maintenance technicians and system administrators will, because of the nature of their job function, be required to share some login accounts as well as those passwords used for management of common system resources and service software. They will also be given administrative and personal login accounts which will allow concurrent logons.
 - b. Temporary login accounts will be created by the NSG for use during the first week of any quarter in a specific classroom. This will allow student users a few days to acquire personal accounts.
 - i. These accounts will be limited to a specific room, but may be used concurrently on as many computers as are in the room.
 - ii. The password for these accounts will not be blank and will comply with strong password recommendations.
 - c. A single, generic local instructor login account and strong password may be created to provide faculty access to the computers in podiums in the electronic classrooms and labs across campus. This account will have local standard user access only.

C. Individual Account Responsibility Exception

1. Login IDs and passwords will not be assigned to a job function or group of individuals, except under the following circumstances:
 - a. Login IDs and passwords will be created for each Associated Student Government position (ASG). This is to provide communications continuity within the student community, no matter which individual student holds any particular position.
 - i. The Login IDs and passwords will be created by the appropriate Information Resources systems administrator and disseminated to the Director of Student Programs, who will be responsible for identifying who is authorized to access the accounts and for advising those students of that information.
 - ii. At the end of Summer quarter, the passwords for each of these accounts will be changed and the new passwords will be disseminated to the Director of Student Programs for distribution to incoming ASG officers.
 - b. Generic login IDs and passwords to the computing equipment used in Television Services will be allowed. This will facilitate student and volunteer access to the specific equipment used in that area to support both curriculum and the delivery of services to the greater community.
 - i. The Login IDs and passwords will be created by appropriate Information Resources systems administrator and disseminated to the Director of Television Services, who will be responsible for identifying who is authorized to access the accounts and for

advising those users of that information.

D. Numeric Password Exception

1. Some systems on campus, such as, SCAN, phone-mail, etc., require only numeric passwords/pass-codes because the system itself is unable to process combinations of characters and numbers. Numeric-only password/pass-codes for these are allowed to be created as exceptions to the "Password Management" standard requirements for selection of strong passwords.
2. Phone-mail or SCAN passwords/pass-codes are exempt from the 120-day requirements of the "Password Management" standard for "Aging."

E. Public Workstation Exceptions

1. Library Media Center

- a. In addition to its services to the campus community, the mission of the Library Media Center (LMC) includes providing library services to the greater community at large. This includes allowing community members otherwise not affiliated with the college to use public computing systems housed in the LMC.
- b. Access by the public to Bellevue College workstations is generally prohibited by the IT security standards and policies. However, because these dedicated workstations are being used to provide an appropriate college service to the community, an exception is being granted to allow their use and to waive the requirements enumerated by the Bellevue College IT security standard addressing "Password Management" for individual account responsibility. The specific exception granted is:
 - i. The public computers in the LMC will be configured to allow logging-on using a generic public login name and password.
 1. LMC personnel will work with the NSG to identify which LMC computers are the public computers covered under this exception, and to create and maintain the public login names and passwords.
 2. The public computers in the LMC will have restricted access to any Bellevue College networks, as determined by the NSG. This access will include limiting access to only Internet, internal database and informational resources, and printing support. Any other access to any Bellevue College networks will not be permitted using these accounts.
 3. LMC personnel will be responsible for communicating the public login names and passwords to appropriate LMC patrons.
 4. This exception does not extend to any office or administrative use workstations in the LMC. Those systems will be expected to comply with all Bellevue College IT Security policies and standards, just as any other campus system.
- c. The computers designated for community use in the LMC are considered public access computers, as defined in Bellevue College policy #5170: Library and Career Center Internet Usage.

2. Career Center

- a. The primary service offered by the Bellevue College Career Center is to provide job information and counseling to both the Bellevue College community and the greater Bellevue community at large. This includes allowing community members otherwise not affiliated with the college to use public computing systems housed in the Career Center. Access by the public to these workstations is generally prohibited by the IT security standards and policies.
- b. However, because these workstations are being used in providing an appropriate service to the community, an exception is being granted to allow their use and to waive the

requirements enumerated by the Bellevue College IT security standard addressing "Password Management." The specific exception granted is:

- i. The public computers in the Career Center will be configured to allow logging-on using a generic public login name and password.
 1. Career Center personnel will work with the NSG to identify which Career Center computers are the public computers covered under this exception, and to create and maintain the public login names and passwords.
 2. The public computers in the Career Center will have restricted access to any Bellevue College networks, as determined by the NSG. This access will include limiting access to only Internet, internal database and informational resources, and printing support. Any other access to any Bellevue College networks will not be permitted using these accounts.
 3. Career Center personnel will be responsible for communicating the public login names and passwords to appropriate Career Center patrons.
 4. This exception does not extend to any office or administrative use workstations in the Career Center area. Those systems will be expected to comply with all Bellevue College IT security policies and standards, just as any other campus system.
- c. The computers designated for community use in the Career Center are considered public access computers, as defined in Bellevue College policy #5170: Library and Career Center Internet Usage.

3. Computer Kiosks

- a. The Director of Computing Services may direct that limited-use computers, generally expected to be used on a temporary basis by individuals who are not network account-holding members of the campus, be configured to work in "kiosk" mode upon startup. This means the computers are automatically logged into the Bellevue College network using a login name and strong password specific to their location, and do not require the user to provide login credentials.
- b. Computers configured as kiosks in **public locations** will have limited access to the services available through the network, as is fitting for their specific purpose. Example of these types of computer include:
 - i. Registration kiosks placed in the Student Services area to allow individuals to apply to the college or register for classes.
 - ii. Internet-only kiosks placed as a convenience for students, such as the North campus cafeteria area and the Main campus Student Programs areas.
 - iii. Informational kiosks.
- c. Computers configured in **classrooms** as kiosks should only be used where it is impractical for students to acquire Bellevue College network credentials prior to class sessions. Kiosked classroom computers may have full access to all Bellevue College networked resources.
 - i. This is generally appropriate for classrooms used by Continuing Education classes.
 - ii. With respect to credit classes, this is appropriate only for the first week of classes during any given quarter.
 - iii. Students may not use classroom computers configured as kiosks except in the presence of a Bellevue College instructor.
- d. Computers configured as kiosks will be placed on virtual networks separate from the

main Bellevue College networks, if possible.

- e. Kiosked computers will be configured to require Bellevue College authorized login credentials if the processes establishing it as a kiosk are bypassed by a user upon startup.

F. Board of Trustees Exception

1. Members of the Bellevue College Board of Trustees are granted Bellevue College login and e-mail accounts to enable them to utilize Bellevue College technology resources while performing their official duties.
2. However, trustees are not standard employees of the college, are infrequently on campus, and do not use their login and/or e-mail accounts in a consistent manner. In addition, the accounts used by individual trustees do not have any special access to resources.
3. Therefore, accounts for the members of the Board of Trustees will be configured to not expire, an exception to the "Aging" section of the "Password Management" standard.

Appendix A – References

1. DIS Technical Bulletin—1.2.18.19, Implementation of a Strong Password Standard for S/390 Userids, November 15, 2001
2. SBCTC-IT Security Standard—Password Management
3. Bellevue College IT Security Standard: Password Management
4. Department of Information Services (DIS) Information Technology Security Policy for Institutions of Higher Education, pursuant to RCW 43.105.200.

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