



IT Security Standard:

Password Management

Introduction

This standard defines the steps needed to implement Bellevue College policy # 5250: *Information Technology (IT) Security* regarding management of all passwords used by staff, faculty and students to utilize the Bellevue College networks and computers. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines minimum acceptable password selection criteria, as well as specific procedures for management of passwords, for all Bellevue College accounts. It is recognized that password authentication, while less than optimal, is still the standard means of ensuring the security of computing systems.

Furthermore, each computing platform provides differing levels of support for securing passwords. It is also recognized that strict adherence to this standard often depends on details specific to a platform's implementation.

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.

Student computing accounts at Bellevue College are automatically covered in the Password Management Exception document.

Business Impact and Risk, Threat and Vulnerability Analysis

Bellevue College uses passwords for the vast majority of its authentication needs. As such, the selection and management of passwords is a critical factor in assuring the security of the computing and communications resources under Bellevue College's responsibility. A significant compromise to password security could put the college instructional and business systems at great risk.

Passwords can be the weakest link in a computer security scheme. Strong passwords are important because password cracking tools continue to improve and the computers used to crack passwords are more powerful. Network passwords that once took weeks to break can now be broken in hours.

Given the high level of dependence on password-based authentication, the most significant threats are:

1. Malicious and/or unauthorized access to controlling components (e.g., routers, DNS, domain controllers)

2. Malicious and/or unauthorized access to data and or processes
3. Theft and/or malicious manipulation of data and/or services
4. Fraudulent use of data and/or services

Given the nature of the asset and the nature of the threat, all risks associated with passwords are very significant and could cause significant loss to Bellevue College.

Standard

A. Introduction

1. Passwords are the primary security mechanism used at Bellevue College to authorize and authenticate use of Bellevue College technology resources. This standard identifies the use of passwords to access the resources that users need to accomplish work duties. Passwords will control logging onto the computer and any Bellevue College network resource.

B. Password Creation

1. All individuals using the Bellevue College Administrative computing network or computing resources will have an authorized account and password to access the systems. This includes any full-time employees, part-time employees, temporary employees, student employees, and non-employee users.
2. Login IDs and passwords will not be assigned to a specific job function or group of individuals unless specifically addressed in the "Password Management Exceptions" document.
3. Prior to receiving a Bellevue College password, an account will be requested by a unit administrator using the "Bellevue College Network Account and E-mail Request" form.
4. Campus users will acknowledge they have read the Bellevue College policies #5150, "Acceptable Use of Bellevue College Networks and Systems" and #5000, "Acceptable Use of Bellevue College Computers."
5. Users will sign the form and acknowledge having read and understood the policies.
6. Unit administrators will sign the form affirming the request for the creation of an account and password.
7. The form will be forwarded to the IR support personnel authorized to create and maintain accounts for action, and stored in a secure location once the account has been created.
8. The user will be notified of the creation of the account in the following ways:
 - a. Distribution of passwords will always be performed in a secure fashion.
 - i. Individuals may pick up their passwords from the accounts manager in Information Resources.
 - ii. Passwords may be distributed by campus mail in a sealed envelope marked CONFIDENTIAL addressed to the authorized individual. The recipient should shred the paper after the information has been distributed.

C. Password Security

1. Passwords are the primary means of authenticating users to computer and network devices within Bellevue College's managed computer systems.
 - a. This is a security measure required to help maintain the integrity of the Bellevue College networks and systems.
2. Passwords will never be shared. Bellevue College employees will not ask for, accept, or use others' passwords. Users alone are responsible for what is done with assigned user name and password.
 - a. One significant exception are IR maintenance technicians and system administrators who, by job function, are required to share some login accounts as well as those passwords used for the management of common system resources and service software.

- b. Employees may also share passwords with Bellevue College technical support personnel, as necessary, to facilitate the support and maintenance of Bellevue College systems. The expectation is that this type of access will be rare and treated sensitively by support personnel.
 - c. Other shared passwords will be enumerated in the "Password Management Exceptions" document.
3. Password controlled logins to the Bellevue College network will be limited to one occurrence only. Concurrent logons will not be allowed unless specifically identified in the "Password Management Exceptions" document.
4. Bellevue College network and computer passwords will never be used for any other purpose (i.e. free e-mail accounts, Web site registration).
 - a. If these other uses are security compromised, the Bellevue College resources could be compromised.
5. If a password becomes known or is suspected to be known by another user, the password will be changed immediately.
6. Passwords will not be written down. A written password is more easily discovered than one committed to memory.
 - a. If this is impossible for some reason (i.e., too many passwords to remember), great care will be taken to protect the written copy. NEVER post passwords on the computer or monitor of a workstation. They should never be left where they can be found during a five-minute rifling of an office.
 - b. If it is necessary to write the passwords down, consider using a software tool to protect password lists. All such tools will be reviewed by the Bellevue College IT Security Administrator and/or the Dean of Information Resources prior to use.
7. Local administrator accounts on computers will have a different password from the user's network logon password and will not use the same password as system administrator accounts.
8. Passwords will not be coded into scripts, job controls, programs, or other places where they can be used to circumvent appropriate authentication or can be read by another person.
9. Passwords for system administration accounts (e.g., Administrative and Student servers, root, administrator, and the router passwords) will be secured in sealed envelopes and stored in a secure location designated by the Dean of Information Resources or authorized designee.
 - a. The Bellevue College IT Security Administrator and/or the Dean of Information Resources will be advised of the storage location and will have complete access to the information.
 - b. This information will be stored in either hard copy or electronic form. Adequate provisions for backup of the information will be made.
 - c. If the storage location is compromised, the Bellevue College IT Security Administrator and/or the Dean of Information Resources will be notified and all system administration account passwords will be immediately changed.
10. Users will be careful when typing passwords. They will make certain no one is looking over shoulders. They will also be courteous to others typing passwords and will not watch as they do so.
11. Users will be careful when saving passwords electronically on computers. Some dialog boxes, such as those for access to Web sites and other connections, present an option to save or remember your password on your computer; never select that option.

D. Password Troubleshooting and Maintenance

1. In an emergency situation, in an effort to troubleshoot problems which may occur with an account, or when the need for an instant reaction to a threat to campus systems is necessary, Bellevue College support personnel will change a user's password without prior notice.
 - a. If feasible, attempts to contact the individual account holder will be made before a password change is instituted.
 - b. The user will be subsequently notified of the change and offered an opportunity to change the password again once the problem is resolved.
 - c. In certain circumstances, password changes or termination are required to be approved by the Vice President of Human Resources (HR). The approval will be obtained in advance of any such changes whenever possible. However, in exigent circumstances, that approval may take place after the action. All such situations will be reported by Dean of Information Resources or authorized designee to the HR Vice President as soon as possible after such action has been taken.
2. To provide support to campus users, the support personnel authorized to change user passwords will include:
 - a. Systems Administrators
 - b. Authorized Help Desk designees
 - c. Anyone specifically authorized and designated by the Dean of Information Resources

E. Passwords Selection

1. Passwords will be at a minimum eight (8) characters long.
2. Passwords will contain a mix of at least three elements from the following four groups. Additional elements may be used, if desired:
 - a. upper-case alphabetic
 - b. lower-case alphabetic
 - c. numeric
 - d. symbols
3. Passwords will not be a common word or name.
4. Passwords will not be a word with a simple alphabetic to numeric substitution.
5. Strictly numeric passwords—such as phone numbers, Student Identification Numbers or Social Security Account Numbers—will not be used as they are very weak.
6. Passwords will not contain any part of a real name or user name or be a variation of the name.
7. A compromised password will be changed by the user or support personnel immediately.

F. Aging

1. Password changes will be required at least every 120 days.
2. Passwords will not be changed more frequently than every seven days. If there is need to change the password more frequently, this will be over-ridden by the appropriate system administrator.
3. Passwords will not be reused more frequently than every five (5) password changes.
4. Any exceptions that may exist to these aging requirements will be enumerated in the "Password Management Exceptions" document.

G. Password Auditing

1. Twice a year, authorized systems administration staff will perform a password policy audit to ensure that users are selecting strong passwords. The systems administrator performing this

audit will provide appropriate protection for the data being analyzed as it is extraordinarily sensitive. The possession of password capture or cracking software by other than specifically designated security and systems administrators is strictly forbidden on the Bellevue College network and will be viewed as an attack against the network.

2. Users whose passwords are found to be weak will be required to change their passwords to new, strong passwords.
3. The Bellevue College IT Security Administrator and/or Dean of Information Resources, for examining trends and basic statistics, will maintain a list of users failing the audit.

H. Automation

1. An automatic "lock-out" mechanism will be in place and will be activated after a maximum of five (5) unsuccessful authentication attempts.
2. Wherever possible, the above policies will be implemented by the operating system or add-on security package and will not be left to the user to enforce compliance. However, this requirement does not relieve the user of the responsibility of maintaining compliance with these standards.

I. Staff Separation

1. When an employee separation occurs, the employee's account will be disabled on the last working day. If the employee had access to accounts other than personal ones (e.g., support, administrator, network), those additional account passwords will be changed no later than the employee's last working day.
2. The Director or Organizational Unit Administrator (OUA) to whom the person reported may choose to have some or all account access disabled prior to the actual separation date. This is especially true in the case of Bellevue College systems and security administrators.
3. The Director or OUA to whom the person reported is responsible for informing Information Resources, through the IR Help Desk, of the employee separation no later than when it occurs (i.e., the employee's last day in the office).

J. Prohibitions

1. Passwords locking the configuration of the computer (such as CMOS) will only be used by technical support personnel, or an authorized designee, when they are required for a specific security purpose. Under no circumstances will they be used by any other Bellevue College employee. Use of such passwords to lock a system will be considered an attempt to thwart Bellevue College control over a computer and will be investigated as an attack on the system.

K. Remedies

1. User accounts and passwords will be disabled immediately by the appropriate systems administrators upon discovery of a significant breach of these standards or of any Bellevue College IT security policies or standards.
 - a. Immediate notification of this action will be made to the Director of the responsible IR unit and the Director or OUA to whom the person reports.
 - b. A report will be made to the Bellevue College IT Security Administrator and the Dean of Information Resources concerning the violation and actions taken.
2. User accounts permanently disabled for security concerns will not be re-enabled without specific permission from the Dean of Information Resources or 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. 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 Policy #5150, "*Acceptable Use of Bellevue College Networks and Systems*"
4. Bellevue College Policy #5000, "*Acceptable Use of Bellevue College Computers*"

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