User Accounts and Passwords

Purpose

User authentication is the means by which Technology resource authorizes a user by verifying that the user provided the correct identity. Bellevue School District (BSD) relies on a combination of User ID and Password to do this. Passwords are a critical part of information and network security. Passwords serve to protect user accounts, but a poorly chosen password, if compromised, could put the entire network at risk. As a result, all employees, students, vendors and contractors of BSD are required to take appropriate steps to ensure that they create strong, secure passwords and keep them safeguarded at all times.

Definitions

1. User Account: The user account is made up of the User ID and password.
2. User: The individual requesting a user account in order to perform work in support of a BSD program or a project, by accessing the KM computer network. This includes system users, though it is recognized that some legacy systems will not support this policy.
3. User ID: Also referred to as a username. A User ID identifies the user on the system and has an associated password.
4. Technology Resources: This includes, but is not limited to, computers, hardware, software, networks, computing laboratories, databases, files, information, software licenses, computer-related contracts, network bandwidth, user ids, passwords, documentation, disks, RD-ROMs, DVDs, magnetic tapes, and electronic communication.
5. Password: A string of characters which serves as authentication of an individual's identity, which is used to define access rights to private or shared data.
6. Strong Password: Strong passwords are constructed of a sequence that contains both upper and lowercase letters, numbers, and special characters, depending on the capabilities of the operating system or application. Typically, the longer the password the stronger it is. Passwords must be unique across all technology resources and not easily tied back to the user, such as: User ID, given name, social security number, telephone numbers, student/employee number, phone or office numbers/extensions, addresses, nicknames, family or pet names, birth date, license plate number, etc.

User Accounts

Password General

1. All users accessing technology resources will have a unique user id and password.
2. Passwords must be changed every 180 days.
3. Old passwords cannot be re-used for a period of 12 months.

4. Users will be notified of password expiration. At this time, users will be prompted to select a new password.
5. All passwords must conform to the guidelines outlined below.
6. Passwords may not be written down, unless stored in an encrypted format.

Password Protection Standards

1. Passwords should be treated as confidential information. No employee/student is to give, tell, or hint at their password to another person, including Technology staff, administrators, supervisors, other co-workers, friends, and family members, under any circumstances. If someone demands your password, refer them to this procedure or have them contact the Technology Department or their teacher/supervisor. Exception: Students can share their passwords with their parents/guardians and are encouraged to do so.
2. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to district resources via the District's IPsec-secured Virtual Private Network or SSL-protected Web site.
3. No user is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form.
4. Passwords used to gain access to the district's systems should not be used as passwords to access non-districts accounts or information (i.e. Personal accounts).
5. If a student/employee either knows or suspects that his/her password has been compromised, it must be reported to the Technology Department and the password changed immediately.
6. The Technology Department may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

Password Reset Procedure

Employees should contact their building Technology Specialists or contact the BSD's Service Center (x4321). The request will be followed up with a return call (if the user is not their physically) to validate the user requesting the change. Upon validation, the password will be set to a new unique password and read over the phone to the user while they are logging in. Passwords are not to be sent via eMail.

Students can have their passwords reset by any classroom teachers or staff using BSD's password reset tool.

Exceptions
Any exception to this procedure must be approved by BSD's Director of Technology or equivalent. Examples: Some systems my require the assignment of passwords by Technology staff or don't support the documented guidelines. The use of **Classroom** and **Testing** accounts are approved to gain quick student access to controlled environments.

Enforcement
Any employee/student who is found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment.

Password Construction Guidelines
Passwords are used to access any number of district systems, including the network, e-mail, the Web, and voicemail. Poor, weak passwords are easily cracked, and put the entire system at risk. Therefore, strong passwords are required. Try to create a password that is also easy to remember.

1. Initial Passwords require the user to reset after the first use.
2. Passwords must contain at least 8 characters.
3. Must be at least 8 characters in length and contain characters from three of the four following categories: Sample: We1come! (Do not use this sample)
   a. English uppercase characters (A through Z)
   b. English lowercase characters (a through z)
   c. Base 10 digits (0 through 9)
   d. Non-alphabetic characters (for example, !, $, #, %)
4. Passwords may not contain your First, Middle or Last name
5. Passwords should not be based on well-known or easily accessible personal information.
6. Passwords should not be words that can be found in a standard dictionary (English or foreign) or are publicly known slang or jargon.

Password Creation Tips:
1. Think of a sentence that you can remember. This will be the basis of your strong password or pass phrase. Use a memorable sentence, such as "My son Aiden is three years old."
2. Check if the computer or online system supports the pass phrase directly. If you can use a pass phrase (with spaces between characters) on your computer or online system, do so.
3. If the computer or online system does not support pass phrases, convert it to a password. Take the first letter of each word of the sentence that you've created to create a new, nonsensical word. Using the example above, you'd get: "msaityo".
4. Add complexity by mixing uppercase and lowercase letters and numbers. It is valuable to use some letter swapping or misspellings as well. For instance, in the pass phrase above, consider misspelling Aiden's name, or substituting the word "three" for the

number 3. There are many possible substitutions, and the longer the sentence, the more complex your password can be. Your pass phrase might become "My SoN Ayd3N is 3 yeeRs old." If the computer or online system will not support a pass phrase, use the same technique on the shorter password. This might yield a password like "MsAy3yo".

5. Finally, substitute some special characters. You can use symbols that look like letters, combine words (remove spaces) and other ways to make the password more complex. Using these tricks, we create a pass phrase of "MySoN 8N i$ 3 yeeR$ old" or a password (using the first letter of each word)

Date: 09.14