

Protecting Your Password Standard

Revision Date: 8-15-05

1. Purpose: User authentication is a means to control who has access to an Information Resource system. Controlling the access is necessary for any Information Resource. Access gained by a non-authorized entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to El Paso Community College (EPCC).

2. Scope: The purpose of the EPCC Password Policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of (EPCC) user authentication.

3. Description: A password is a string of characters which serves as authentication of a person's identity, which may be used to grant, or deny, access to private or shared data. A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically the longer the password the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about you such as a birth date, social security number, and so on.

- All passwords, including initial passwords, must be constructed and implemented according to the following EPCC Information Security rules:
 - ❖ it must be routinely changed
 - ❖ it must adhere to a minimum length as established by EPCC Information Security
 - ❖ it must be a combination of alpha and numeric characters
 - ❖ it must not be anything that can easily tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc.
 - ❖ it must not be dictionary words or acronyms
 - ❖ password history must be kept to prevent the reuse of a password
 - ❖ it should use both lowercase and uppercase alphabetic characters
- Stored passwords must be encrypted.
- User account passwords must not be divulged to anyone. EPCC Information Security and Information Security contractors will not ask for user account passwords.
- When used, security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with EPCC.
- If the security of a password is in doubt, the password must be changed immediately.
- Administrators must not circumvent the Password Standard for the sake of ease of use.
- Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hardcoded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the EPCC Information Security Manager. In order for an exception to be approved there must be a procedure to change the passwords.
- Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.

- Helpdesk password change procedures must include the following:
 - ❖ authenticate the user to the helpdesk before changing password
 - ❖ change to a strong password
 - ❖ the user must change password at first login
- In the event passwords are found or discovered, the following steps must be taken:
 - ❖ Take control of the passwords and protect them
 - ❖ Report the discovery to the Information Technology Help Desk
- Transfer the passwords to an authorized person as directed by EPCC
- Passwords must be changed at least every 90 days
- Passwords must have a minimum length of 8 alphanumeric characters and may include special characters
- Passwords should contain a mix of upper and lower case characters and must have at least one (1) numeric character and at least one (1) alphabetic character. The numeric characters must not be at the beginning or the end of the password. Special characters provide extra security and should be included in the password where the computing system permits. The special characters are these: ! @ # \$ % ^ & * _ + = ? / ~ ` ; : , < > | \)
- Passwords must not be easy to guess and they:
 - must not be your Username
 - must not be your employee number
 - must not be your name
 - must not be family member names
 - must not be your nickname
 - must not be your social security number
 - must not be your birthday
 - must not be your license plate number
 - must not be your pet's name
 - must not be your address
 - must not be your phone number
 - must not be the name of your town or city
 - must not be the name of your department
 - must not be street names
 - must not be makes or models of vehicles
 - must not be slang words
 - must not be obscenities
 - must not be technical terms
 - must not be school names, school mascot, or school slogans
 - must not be any information about you that is known or is easy to learn (favorite - food, color, sport, etc.)
 - must not be any popular acronyms
 - must not be words that appear in a dictionary
 - must not be the reverse of any of the above
- Passwords must not be reused for a period of one year
- Passwords must not be shared with anyone

- Passwords must be treated as confidential information
- Combine short, unrelated words with numbers or special characters. For example:
eAt42peN
- Make the password difficult to guess but easy to remember
- Substitute numbers or special characters for letters. (But do not just substitute) For example:
 - livefish - is a bad password
 - L1veF1sh - is better and satisfies the rules, but setting a pattern of 1st letter capitalized, and i's substituted by 1's can be guessed
 - !lV3f1Sh - is far better, the capitalization and substitution of characters is not predictable

4. Enforcement: Violation of this standard may result in disciplinary action in accordance with El Paso Community College policy and procedures. If you need clarification of this standard, call the Information Security Office at 831-6312, or e-mail richardb@epcc.edu, from the office of the Vice President for Information Technology/Chief Information Officer.