BRIDGEVALLEY COMMUNITY & TECHNICAL COLLEGE

PASSWORD

Date approved by cabinet: March 8, 2023
Effective date: April 20, 2023
Expiration date (5 years from effective date if not renewed): April 20, 2028

Section 1. Policy Statement

1.1. BridgeValley Community and Technical College (College Authorized Users shall use passwords as a primary method of protecting access to College systems. It is imperative that passwords are strongly constructed and used in a manner to prevent account compromise. Authorized Users will protect their passwords by adherence to best practices for password security.

Section 2. Scope

2.1. This policy applies to all College accounts accessing College network and systems.

Section 3. Password Management

3.1. Authorized Users' College Domain Account Passwords will be initially issued by the IT Department in compliance with the Account Management Policy.

3.1.1. Initial usernames and passwords will be relayed to students via their acceptance letter.

3.1.2. Initial usernames and passwords will be relayed to faculty and staff via their supervisor.

3.1.3. A guest account password will be relayed directly to the visitor of the College upon request.

3.2. All user account passwords shall be strong, preferably passphrases which are at least 8 characters long or randomly generated, that must meet the following:

3.2.1. Minimum of eight (8) characters in length, and

3.2.2. Meet password complexity requirements by containing characters from at least three out of four categories:

3.2.2.a. English uppercase characters (A – Z)

3.2.2.b. English lowercase characters (a - z)

3.2.2.c. Base 10 digits (0 – 9)

3.2.2.d. Non-alphanumeric characters (For example: !, $, #, or %)

3.2.3. Exclude only words that may be found in any dictionary, language, slang, dialect, jargon, etc., and

3.2.4. Not contain three or more consecutive characters from the user's first name, last name, or username.

3.2.5. Not be solely based on easily guessed personal information, names of family member, pets, etc.

3.2.6. Not include consecutive characters (e.g., abc or 123).

3.2.7. Not include personal or financial information such as Social Security or credit card numbers.

3.2.8. Passwords must be unique. As such, eight (8) unique passwords must be selected before a password can be reused.

3.3. Service account passwords shall follow the following guidelines:

3.3.1. Must be created and stored in IT Department approved password vault.

3.3.2. Must be randomly generated.

3.3.3. Minimum of 20 characters in length.

3.3.4. Must contain characters from all four of the following categories:

3.3.4.a. English uppercase characters (A - Z)

3.3.4.b. English lowercase characters (a - z)

3.3.4.c. Base 10 digits (0 - 9)

3.3.4.d. Non-alphanumeric characters (For example: !, $, #, or %)

3.4. If a password is suspected to have been compromised, it should be changed immediately and the incident reported to the IT Department.

3.5. Passwords must never be left in a location that can be readily obtained and utilized by another individual to Authenticate to a College system.

3.6. Passwords must never be stored electronically in plain text such as in a document, spreadsheet, or .txt file.

3.7. Never use the same password for multiple College accounts and/or personal accounts.

3.8. Passwords may be stored electronically in an encrypted Password Vault.

Section 4. Password Change Requirements

4.1. Authenticated User’s College Domain Account password shall be changed every 180 days.

4.2. Shared account and Service account passwords shall be changed upon employee turnover in the department in which the employee had access to the password for the account.

Section 5. System Administration of Passwords

5.1. Server systems Administrator passwords shall be stored in a minimum of two locations. Copies of the current passwords shall be stored on an encrypted file on the IT Department’s Administrative File Server, the password vault. The second copy shall be stored in an encrypted file on a separate IT Department Administrative File Server. Any additional electronic files must be encrypted. The IT Department will designate individuals that will have access to the password key phrases that protect the encrypted password files.

5.2. Use of default passwords for system accounts is prohibited.

5.3. College Domain Account must be used for Authentication. Local accounts should only be used for Authentication when use of Domain Account is technically not possible.

5.4. College systems must automatically lock after no more than ten (10) unsuccessful, consecutive logon attempts to deter Brute Force Attacks.

5.5. Passwords must be protected in transit using industry-standard cryptographic protections.

5.6. Passwords must be hidden by default during login process.

5.7. Temporary passwords must be set to change upon first logon.

5.8. Passwords of Compromised accounts must be reset in a timely manner or require users to reset their own passwords in situations where continued use of a password creates risk of unauthorized access to the computing account or resource.

Section 6. Definitions.

6.1 Authenticate -— The process of providing credentials to prove an individual has permission to access a particular system or file.

6.2. Authorized User – College faculty, staff, students, and guests that have been granted permission to access the College system accounts through the issuance of a username and password.

6.3. Best Practice – A method or technique that has consistently shown results superior to those achieved with other means, and that is used as a benchmark.

6.4. College Domain Account – An account stored in a centralized directory service used for authenticating against and authorizing access to College network and systems.

6.5. Compromised - an account that has been maliciously broken into and could be used by an unauthorized individual for criminal reasons.

6.6. Password Strength – A measure of the effectiveness of a password in resisting guessing and brute-force attacks. In its usual form, it estimates how many trials an attacker who does not have direct access to the password would need, on average, to guess it correctly. The strength of a password is a function of length, complexity, and unpredictability.

6.7. Password Vault -— An encrypted, password protected, password management system, (e.g., KeePass, Bitdefender, etc.).

6.8. Service Account - User account that's created explicitly to provide a security context for services that are running on various operating systems.