Blue Mountain Community College

Administrative Procedure

Procedure Title: **Password Policy**
Procedure Number: **04-2019-0001**
Board Policy Reference: IV.A. General Executive Direction

Accountable Administrator: **Chief Operations Officer**
Position responsible for updating: **Chief Technology Officer**
Original Date: **01-22-2020**
Date Approved by College Planning Council: 12-14-2022
Authorizing Signature: *signed original on file*
Dated: **12-14-2022**
Date Posted on Web: **01-24-2023**
Revised: **12-14-22**
Reviewed: 12-22

Purpose/Principle/Definitions:

Purpose

The purpose of this procedure is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.
Passwords are an important aspect of information technology systems security and the protection of information assets. A poorly chosen password may result in unauthorized access and/or exploitation of Blue Mountain Community College's (BMCC) resources. All users, including staff, faculty, student/temporary employee, and partners with access to BMCC systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Principle

This procedure includes users who have or are responsible for at least one BMCC system, application, or information assets, independent of whether you are an end user or a system administrator for that system or application.

Password Requirements

Password requirements are as follows:

- At least one lower case letter [a-z]
- At least one upper case letter [A-Z]
- At least one numeral [0-9]
- At least one special character [!@#^&*?-]
- Minimum of 10 characters
- Maximum of 64 characters

Password Examples:

- EmId2cohcwc! (Every morning I drink 2 cups of hot coffee with cream!)

Long password:

- I eat 3 carrots each day!

Password Lockout and changes:

- Password attempts: at least 4 attempts allowed before lockout
- Passwords changes: Minimum of every 365 days

Password History

- Previous passwords should not be re-used.

Password Protection

- Use a unique password for each online account/service
- Passwords must not be shared with anyone. All passwords are treated as sensitive, confidential BMCC information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not share BMCC passwords with anyone, including administrative assistants, managers, co-workers while on vacation, and family members.
- Do not write passwords down and store them in any unsecured location in your office.
- Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Do not use the same passwords on college systems as you use on your personal accounts

If you suspect unauthorized access to your account or think your password has been compromised, change your password immediately and report the incident to the IT helpdesk.

Additional Security Protection

- Multi-Factor Authentication for added security.

Administrative Procedure Compliance

Compliance Measurement

Information Technology will verify compliance to this procedure through various methods, including but not limited to, business tool reports, internal and external audits, and provide feedback to the Chief Technology Officer.

All users must take all mandatory security and compliance training as directed by the college, and within the prescribed frequency.

Exceptions

The Chief Operating Officer must approve any exception to the Procedure in advance.

Non-Compliance
An employee found to have violated this Procedure may be subject to disciplinary action, up to and including termination of employment. BMCC reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. To the extent permitted by law, BMCC reserves the right not to defend or pay any damages awarded against employees, faculty members or partners that result from violation of this Procedure.

Definitions:

ISO: International Organization for Standardization

Information Asset: Any BMCC data in any form, and the equipment used to manage, process, or store BMCC data, that is used in the course of executing business, regardless of location where the data is stored - on-campus, in an off-site, or cloud environment.

MFA: Multi-factor authentication (MFA) is a layered approach to securing physical and logical access where a system requires a user to present a combination of two or more different authenticators to verify a user's identity for login.

NIST: National Institute of Standards and Technology.

Partner: Any non-employee or contractor of BMCC who is contractually bound to provide some form of service to BMCC.

Password: An arbitrary string of characters that is used to authenticate the user when he/she attempts to log on, to prevent unauthorized access to his/her account.

SSO: Single sign-on is an authentication method that allows users to sign in using one set of credentials to multiple independent software systems.

User: Any BMCC staff, faculty member, student/temporary employee or partner who is authorized to access any BMCC electronic information resource.