Standard for Authentication, Accounts, and MFA

Parent Policy:	*Use of Information Technology Resources*		
Standard Sponsor:	College Information Officer		
Standard Contact:	Manager, IT Security		
Stakeholders:	Okanagan College Application Owners		
Approved by:	College Information Officer		
Effective Date:	19-January-2024		
Last reviewed:	19-January-2024	Scheduled review date:	19-January-2025

1. Introduction

1.1 User accounts control access to College information and systems and as such they must be effectively protected against unauthorized access.

1.2 This document defines standards that College staff must comply with when securing these accounts.

2. Account Protection Requirements

2.1 All user accounts must be secured with:

a) passphrases or passwords that follow the Passphrase and Password standard; and

b) multifactor authentication; or

c) private keys (e.g. X.509 certificates or SSH Keys) that are generated using should use strong algorithms.

2.2 Where technically possible, College systems must enforce password complexity rules in accordance with the Passphrase and Password standard.

2.3 Where technically possible, servers and software applications must use pre-shared keys and the most secure connection method supported, (e.g. modern OATH vs legacy SMTP) when communicating between systems, and where possible, administration accounts must be protected by Multi-Factor Authentication (MFA).

2.4 Users who receive new accounts or who require a replacement password must be forced to set or change the password upon first login.

2.5 Account activation or password reset links, and temporary passwords must be transmitted to users in a secure manner.

a) Where possible, activation and registration links should be configured to expire after 7 days.

b) Password reset should leverage multi-factor authentication or have password reset links expire after 24 hours.

2.6 Procedures must be established to verify the identity of a user prior to providing a new, replacement or temporary password for an account. Identification validation procedures must follow one of the following standard practices, listed in order of preference:

a) Multi-factor authentication application push to the user's multi-factor authentication device that must be approved by the user;

b) In-person visit by the user to present valid photo identification, preferably College or government-issued;

c) Validation of answers to three questions unique to the user's account and/or status to prove identity.

2.7 Default vendor accounts (where possible) and passwords must be changed or disabled during the installation of systems or software. New passwords must meet College password standards and use MFA where possible.

3. Admin and Privileged Access Accounts

3.1 Admin and privileged access accounts must be secured in compliance with the Passphrase and Password Standard and include the following additional protections:

a) Increased password length to include a minimum of 16 characters.

b) Daily multifactor authentication.

4. Service and API Accounts with no Multi-Factor Authentication

4.1 Service and API accounts must be secured in compliance with the Passphrase and Password Standard and include the following additional protections:

a) Increased password length to include a minimum of 25 characters.

b) Passwords changed annually.

c) Passwords never stored in code repository, spreadsheets/csv, or plaintext config files.

5. Authentication System Requirements

5.1 Where possible, all user accounts should be centrally controlled in Entra ID

a) Login and authentications systems should use Entra ID for Single Sign On

b) Where not possible, work with IT Security to identify the most appropriate authentication source.

5.2 Authentication systems for user accounts must be adequately protected from password cracking using at least one of the following methods:

a) Progressive Account Lockout: the account is locked for a period of time if an incorrect number of passwords/passphrases is entered over a specified time period (for example, if an incorrect password/passphrase is entered 10 times within a 30 minute window, the account will be locked for 30 minutes). Repeated attempts increase the lockout time exponentially, and/or

b) each time an incorrect password/passphrase is entered, the system introduces a delay before providing the failure response; this delay increases as the failed login attempts continue but will reset once the user successfully logs in (for example, the delay period could begin at 100 milliseconds, and double after each subsequent failed login).

5.3 Authentication systems must not store account passwords in clear text. Where possible, passwords should be stored using a strong cryptographic hash and salted.

5.4 Where possible, authentication systems should support the use of a banned password list, and not allow Users to set easily guessable passwords from the banned password list.

5.5 Where possible, authenticated application sessions must timeout as follows, after which Users must reauthenticate to continue an existing session or establish a new session:

a) after a maximum session length of 12 hours; and

b) where reasonable, after 30 minutes of User inactivity.

History / Revisions

Date	Action
2024-04-29	*New Standard Approved by: College Information Officer*