Internal Policies and Procedures of the Utah State Board of Education	
Policy #	05-04
Subject:	System and Application Login and Authentication
Date Approved	April 26, 2022
Policy Owner's Title	Deputy Superintendent of Operations
Policy Officer's Title	Chief Information Security Officer
References: NIST Special Publication 800-63-3 USBE Information Security Policy	

1) Purpose and Scope

a) The goal of login security should be to enforce good habits and strong security, as well as create a user experience that encourages implicit safe behavior.

b) In all new systems and applications, login and authentication security should be built to at least the minimums stated in this document. For systems that exist prior to this document, every effort should be made to bring their login and authentication security as close to this document as possible.

2) Policy

a) Multifactor Authentication (MFA)

i) MFA must be enabled wherever possible for systems requiring a username/password combination for authentication.

(1) Microsoft Office 365, Google, and/or Active Directory Single Sign-on (SSO) should be implemented for system authentication whenever possible to facilitate inheritance of existing MFA authorizations

(2) Some systems cannot implement MFA due to system shortfalls and/or offline use. Users should implement some other method of two-step authentication or password complexity, if possible.

ii) Authorized MFA utilizes the following one-time password solutions:

(1) Time-based One Time Password (TOTP) – A secret key and the current time are hashed into a one-time password. Each password is valid until it is used.

iii) Authorized forms of MFA are listed below in order of preference:

(1) Hardware Token – physical devices used to generate verification codes.

(a) Connected tokens: Tokens that must be physically connected to the computer with which the user authenticates (e.g., Smartcards, YubiKeys, etc.). Authentication information is transmitted to the system from the token directly via USB or other means.

(b) Contactless tokens: Tokens that are connected to the computer using a wireless protocol, usually Bluetooth or Near-field communication (NFC) (e.g., HID ProxKey devices, etc.).

(2) Software Token – These tokens are stored on the user's computer or mobile device (e.g., Google Authenticator, Microsoft Authenticator, Authy, etc.).

    - (3) One-time passwords through Messaging: Passcodes can be sent from a centralized server to the user via SMS text message or email.
  - iv) Users are authorized to allow web browsers to cache their MFA authorization (e.g., “Remember my answer for 30 days”, etc.). Cached MFA authorizations should not exceed 90 days and are not allowed when performing sensitive actions.
    - (1) Sensitive actions include, but are not limited to:
      - (a) Changing passwords or security questions answers.
      - (b) Changing the email address associated with an account.
      - (c) Establishing MFA account configurations.
      - (d) Performing a system administrative function which requires elevated privileges.

b) Password Security

- i) Password authentication is required for all systems which do not support hardware tokens.
- ii) Passwords must meet the length and complexity requirements identified below.
  - (1) Unique passwords are required for systems that do not support MFA and must be changed every 90 days to mitigate compromises.
- iii) Periodic password resets are not required for MFA enabled accounts.
  - (1) Passwords should be immediately reset if suspected of being compromised.

c) Password Creation

- i) Unique password for each system is recommended, unless explicitly mandated when MFA is not available
- ii) Passwords should be created with a large number and diverse set of characters to mitigate potential compromises. The minimum password length and complexity requirements are defined below:
  - (1) Passwords must be at least eight characters in length utilizing at least one uppercase letter, lowercase letter, number, and special character. We encourage the use of longer passwords as the password length is the preferred industry method for alleviated password compromises.
  - (2) User should restrict words and patterns that cybercriminals are likely to guess, including dictionary words, repetitive or sequential strings, passwords taken in prior security breaches, variations on the site name and commonly used passphrases.
  - (3) The system should allow the use of all characters during password creation, including Unicode and whitespace, whenever possible.
  - (4) A maximum character limit for all system passwords must be set. Character limits should be set to 64 characters or longer if supported.

d) Password Storage

i) Passwords should be committed to memory whenever possible and should only be stored in a secured manner.

(1) Information Technology will maintain a list of approved password vaults authorized for storing credentials on USBE computers and systems.

(a) Password vaults will be protected with a master password and use AES-256 encryption and SHA-256 hashing, at a minimum.

3) Change History

Date	Version	Author	Changes Made / Section(s)
July 12, 2021	0.1.0	Patrick Hawkins	Initial Draft
February 18, 2022	0.1.1	Patrick Hawkins	Document Reviewed and Updated