Internal Policies and Procedures of the Utah State Board of Education	
Policy #	05-04
Subject:	System and Application Authentication
Date Approved	February 21, 2024
Policy Owner's Title	Chief Information Security Officer
Policy Officer's Title	Deputy Superintendent of Operations
References: NIST Special Publication 800-63-3 NIST Special Publication 800-132 USBE Information Security Policy	

1) Purpose and Scope

a) The goal of login security should be to protect accounts from unauthorized access, while also not affecting user experience in a way that causes adverse habits. Examples include creating physical copies of sign in information, reusing passwords, etc.

b) The purpose of this policy is to guide system owners and developers on permittable user login options.

c) 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) 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 Multifactor Authentication (MFA) and must be changed every 90 days to mitigate compromises.

iii) Periodic password changes are not required for MFA enabled accounts.

iv) To protect against system password compromises,

(1) Passwords should be immediately changed if suspected of being compromised by suspicious activity, third party lists of compromised accounts, or other indicators.

b) Multifactor Authentication

i) MFA is to be used in tandem with traditional username and password logins.

ii) MFA must be enabled wherever possible for systems authentication.

(1) All systems developed after the approval of this document must utilize MFA for all accounts.

(2) Single sign-on (SSO) should be implemented through Microsoft Office 365, Google, and/or Active Directory for system authentication whenever possible.

iii) All administrative access accounts must utilize MFA where possible.

iv) MFA is required for remote network access.

v) 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 connect to devices wirelessly (e.g., Radio-frequency identification (RFID) cards, Bluetooth tokens, etc.).

(2) Software token: Tokens that 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 via SMS text message or email.

vi) Authorized MFA can utilize 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.

(2) Mobile Push: The user is sent a notification to a mobile device using the most secure communication channel available.

(3) Fast Identity Online (FIDO): A set of standardized authentication protocols intended for password-less authentication. These protocols include: FIDO2, Universal Authentication Framework (UAF), and Universal Second Factor (U2F).

vii) MFA authorizations may be cached for up to 90 days. MFA caching is 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.

c) Password Creation

i) Passwords should be created with an emphasis on long character strings to mitigate password cracking and brute force attempts. The minimum password length and complexity requirements are defined below:

(1) Passwords must have a character length of at least:

(a) 8 characters if MFA is in use.

(b) 14 characters if MFA is not in use.

(2) A maximum character length for all system passwords must be set. Character limits should be set to 64 characters or longer if supported.

(3) Specific character requirements besides length should be avoided when possible.

(a) If this is not possible, utilizing at least one uppercase letter, lowercase letter, number, and special character.

(4) Words and patterns that are likely to be guessed should be restricted. This includes:
   (a) Dictionary words.
   (b) Repetitive or sequential strings (e.g. 'aaaaaa', '1234abcd', '1qaz2wsx').
   (c) Previously used passwords.
   (d) Context-specific words, such as the name of the service, the username, and derivatives thereof.
   (e) Commonly used passphrases.

(5) The system should allow the use of all characters during password creation, including Unicode and whitespace, whenever possible.

ii) When a created password is rejected by a system; clear, meaningful and actionable feedback should be given (e.g., when it appears on a "blacklist" of unacceptable passwords or has been used previously).

d) Password Storage

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

(1) Password vaults will be protected with AES-256 encryption and SHA-256 hashing or better.

ii) All systems storing login information shall store password hashes with a salt to mitigate inadvertent disclosure.

(1) The salt shall be at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes.

(2) Passwords shall be hashed with a one-way key derivation function.
   (a) Examples of adequate hashing functions include:
      (i) Password-Based Key Derivation Function 2 (PBKDF2)
      (ii) Balloon
      (iii) Argon2

e) System Inventory

i) An inventory of USBE authentication and authorization systems, including those hosted on-site or at a remote service provider, must be kept and maintained.

(1) The inventory must be reviewed and updated at least annually.

f) System Authentication Waiver

i) Any system unable to meet the requirements of this policy, a waiver must be submitted and approved by the Information Technology Director and the Chief Information Security Officer.

(1) Authentication Waivers must be renewed yearly at a minimum.

3) Definitions

a) Hashing: The mathematical process of transforming any given key or a string of characters into a different string of characters.
b) Salt: a random string of characters added to a password before hashing.
c) Unicode: a text encoding standard maintained by the Unicode Consortium. Its purpose is to support written text in all major writing systems.

4) 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
April 6, 2022	0.1.2	Patrick Hawkins	Document Updated
July 20, 2022	0.1.2	Patrick Hawkins	Document Updated
October 19, 2022	0.1.2	Patrick Hawkins	Document Updated
February 1, 2023	0.1.3	Patrick Hawkins	Document Updated
June 28, 2023	0.1.4	Patrick Hawkins	Updated Section D