Administrative Regulation 7228 INFORMATION TECHNOLOGY - AUTHENTICATORS

Responsible Office: Office of Information Technology

PURPOSE

The Superintendent has adopted this Administrative Regulation to establish Multi-Factor Authentication (MFA) guidelines related to authenticators and passwords, in the Washoe County School District (District).

DEFINITIONS

1. "Authentication" refers to the process or action of verifying the identity of a user or process.
2. "Authentication Systems" refers to products, applications and platforms that manage data and allows entities to identify, authenticate, and authorize access to digital resources.
3. "Authenticators" refers to the means used to confirm a user's identity during digital authentication. Authenticators may be known factors (passwords), possessed factors (hardware or software tokens), or biometric factors (personal physical characteristics).
4. "Multi-Factor Authentication" refers to an authentication method that requires the user to provide two or more verification factors to gain access to a resource.
5. "Password/Passphrase" refers to a user-known factor, commonly a string of characters, that allows a user to access a computer system or service.
6. "Password Age" refers to the amount of time that a password remains valid. Password age is typically represented in days.
7. "Password Complexity" refers to password composition with the inclusion of additional length or character sets designed to prevent disclosure through automated means.
8. "Password History" refers to the amount of unique new passwords that must be associated with a user account before an old password can technically be reused.

REGULATION

1. All District personnel with access to District data and Information Systems including employees, contractors, and volunteers must adhere to defined standards and guidelines regarding passwords and authenticators.

2. Securely choosing and protecting passwords can protect District IT Resources from compromise. Voluntarily disclosing, sharing, or using generic accounts and passwords to access District resources is a serious security risk that undermines non-repudiation and may enable bad actors to attack the confidentiality, integrity, and availability of District resources. While some accounts may not have direct access to sensitive information, compromised accounts may be used to gain access to sensitive data.

3. This Administrative Regulation establishes standards for the following password settings on District IT systems:

    a. Authentication Systems;

    b. Multi-Factor Authentication (MFA);

    c. Password Creation Standards;

        i. Password Length;

        ii. Password Complexity;

        iii. Password History;

        iv. Minimum password age;

        v. Maximum password age; and

    d. Password Protection Standards.

4. Authentication Systems

    a. The District manages, through centralized systems, user and administrator accounts, passwords, and authenticators, whenever possible to ensure proper standards enforcement and IT Security response in the event of a security breach.

    b. The Office of Information Technology maintains an inventory of the enterprise's authentication and authorization systems, including those hosted on-site and by remote service providers.

5. Multi-Factor Authentication (MFA)

    a. All user accounts shall have MFA enabled and implemented where practicable;

    b. MFA adds a two-step verification to user authentication using a second factor (e.g., code sent a cell phone, hardware token) in conjunction with a username and password;

c. At a minimum, MFA must be used for:

    i. Externally exposed applications;

    ii. Remote network access including VPN; and

    iii. Administrative Access to Information Systems.

6. Password Creation Standards

    a. Passwords must:

        i. Be unique;

        ii. Have a minimum of 12 characters; and

        iii. Be complex, composed of 3 of the following 4-character sets:

            1) English uppercase characters (A – Z);

            2) English lowercase characters (a – z);

            3) Numerals (0 - 9);

            4) Special characters (such as ! @ # $ % ^).

    b. Passwords should not contain any of the following:

        i. Familiar names that relate to you personally including the names of family, pets, friends, or co-workers, etc.;

        ii. Sensitive personal information such as birthdays, addresses, phone numbers, or social security numbers;

        iii. Computer terms and names, commands, sites, companies, hardware, or software;

        iv. The names of the District (WCSD, Washoe) schools, sites, departments, or mascots or any derivation, or;

        v. Simple words or numbers, or repeatable patterns such as aaabbb, qwerty, zyxwvuts, 123321;

    c. Passwords must not be changed to any previously used passwords or modified versions of previously used passwords;

    d. Password history will be set to the maximum of 25. The system will "remember" the last 24 passwords used, not allowing any repeat of those passwords;

e. Minimum password age will be set to 1 day; and

f. Maximum password age will be set to 1 year (365 days).

7. Password Protection Standards

   a. All passwords must be treated as Confidential District Information;

   b. Users must not use the same password for District accounts as for other non-District accounts (e.g., personal email, online banking, online services). Passwords compromised from other systems might be used to access District resources in the event of a third-party breach;

   c. Users must not:

      i. Write down their passwords including writing down a password on a sticky note and placing it under a keyboard or on a monitor to remember it;

      ii. Provide their individual passwords to anyone;

      iii. Reveal a password in an email message;

      iv. Talk about a password in front of others;

      v. Hint at the format of a password (e.g., my family name);

      vi. Reveal a password on questionnaires or security forms;

      vii. Share a password with family members;

      viii. Reveal a password to co-workers while on vacation;

   d. If an account or password is suspected to have been compromised or a password was inadvertently or intentionally revealed, users must report the disclosure to the Office of Information Technology, IT Security Team;

   e. Users should avoid using the "Remember Password" feature of applications (e.g., Internet Explorer, Chrome, Firefox, etc.);

   f. Users must not store passwords in a file on ANY computer system (including phones and tablets) without encryption; and

   g. For assistance with resetting passwords, users can contact the IT Customer Help Desk.

8. Exceptions

    a. Operational needs may necessitate accounts to be created that do not adhere to these standards. These exceptions must be requested and approved through the Office of Information Technology, IT Security Department.

LEGAL REQUIREMENTS AND ASSOCIATED DOCUMENTS

1. This Administrative Regulation reflects the goals of the District's Strategic Plan and aligns/complies with the governing documents of the District, to include:

    a. Board Policy 7205, Information Technology – Data Access Policy; and

    b. Board Policy 7210, Information Technology Services and Operations;

REVISION HISTORY

Date	Revision	Modification
07/19/2022	1.0	Adopted