AP 3721 District Password Procedure

1.0 Passwords are an important aspect of computer and information security. They constitute the front line of protection for user accounts. An easily guessed password may result in data breaches that damage the reputation and/or create great financial exposure for the District. All students and employees (including third parties such as contractors and/or consultants who are provided with authorized access to NOCCCD systems) have a shared responsibility to ensure they are following the procedures in this document.

2.0 **Purpose**

2.1 The purpose of this administrative procedure is to establish a standard for the creation of strong passwords, and the ongoing protection of those passwords. This document further details the implementation of the password provisions of AP 3720, Computer and Electronic Communication Systems.

3.0 **Scope**

3.1 The scope of this administrative procedure includes all personnel and students who have or are responsible for an account (or any form of access that supports or requires a password) on any system (including cloud and Software as a Service [SaaS] accounts) which resides at or is used by any entity or entity acting on behalf of the District. This procedure applies to all information systems and technology including all networks, equipment, servers, end points, and any other Information Technology service involved in any operation onsite or remote.

4.0 **Procedures**

4.1 Passwords are used for various purposes at the District. Some of the more common uses include user level accounts (computer login), web accounts, email accounts, voicemail, and local logins.

4.2 Password construction requirements include the following:

4.2.1 Be a minimum length of ten (10) characters on all systems;

4.2.2 Not contain the username or name of the user;

4.2.3 Not be transmitted in the clear or plaintext outside the secure location;

4.2.4 Not be displayed when entered;

4.2.5 Not contain repeating characters (e.g. pass10241024);

4.2.6 Not contain characters in sequence (e.g. 12345 or qwerty).

4.3 Multi-Factor Authentication (MFA), also referred to as two-factor authentication (2FA), is a security enhancement that allows users to present two pieces of evidence—otherwise known as credentials—when logging in to an account. Credentials fall into any of the following three categories:

AP 3721 District Password Procedure

4.3.1 something you know (like a password or PIN);

4.3.2 something you have (like a smart card, authenticator application or physical token);

4.3.3 something you are (like your fingerprint - also known as biometrics);

4.4 MFA will be enabled for all accounts accessing the student information system (Banner), network resources, servers, endpoints, or any other technology that could compromise any of those systems.

4.4.1 Students, faculty, and staff will have the ability to self-select their choice of receiving an MFA token. In order of most secure to least secure these are:

4.4.1.1 Mobile authenticator;

4.4.1.2 Physical key/token;

4.4.1.3 Email;

4.4.1.4 SMS.

4.4.2 MFA tokens will not be required while using a device connected to the campus network.

4.4.3 MFA tokens will be required upon first sign-in on any new device.

5.0 **Password Protection Standards**

5.1 Passwords should not be shared. All passwords should be treated as personal and confidential information. The District recommends the use of a password management tool to generate and store personal passwords.

5.2 Examples of “do nots” regarding passwords. This is not an exhaustive list and may be modified to ensure timely best practices.

5.2.1 No Staff member will ever ask for your password;

5.2.2 Do not reveal a password over the phone to anyone;

5.2.3 Do not request someone’s password;

5.2.4 Do not share your password with a co-worker, supervisor, subordinate, or assistant. Do not reveal a password to a fellow student or friend;

5.2.5 Do not reveal a password in electronic communication (email, text, etc.);

5.2.6 Do not talk about a password in front of others;

5.2.7 Do not hint at the format of a password (e.g. “my family name”);

AP 3721 District Password Procedure

5.2.8 Do not reveal a password on questionnaires or security forms;

5.2.9 Do not share a password with family members;

5.2.10 Do not write passwords down and store them anywhere in your office;

5.2.11 Do not store passwords in a file on ANY computer or information system that is unencrypted;

5.2.12 Do not forget to log off when using a shared computer on the college campus (e.g. public space, lab, library, classroom, etc.)

5.3 Poor, weak passwords that are easily compromised contain less than ten (10) characters or a common or familiar word such as:

5.3.1 Birthdays and other personal information such as address and phone numbers, children's names, etc. that are easily discoverable;

5.3.2 Word or number patterns (e.g. aaabbb, qwerty, zyxwvuts, w3e4r5);

5.3.3 Any of the above spelled backwards;

5.3.4 Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

6.0 If someone demands a password, refer them to this document or have them call the District Information Services office for further clarification.

7.0 If an account or password is suspected to have been compromised, report the incident to your Academic Computing Department or the District Information Services office and immediately change all passwords.

See Board Policy 3720, Computer and Electronic Communication Systems; Administrative Procedure 3720, Computer and Electronic Communication Systems; and Administrative Procedure 6365, Accessibility of Information Technology.

Date of Adoption: April 25, 2022 District Consultation Council