North Orange County Community College District
Password Guidelines

Adopted and Approved by
District Information Security Subcommittee

A Subcommittee of Technology Coordinating Council
10.20.2020

1.0 Overview

Passwords are an important aspect of computer and information security. They constitute the front line of protection for user accounts. A poorly chosen password may result in data breaches that damage the reputation of the District 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 guidelines in this document.

2.0 Purpose

The purpose of this guideline 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 AP3720.

3.0 Scope

The scope of this guideline 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 North Orange County Community College District. This guideline 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 Guidelines

4.1 Guidelines

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

Password Construction Requirements

i. Be a minimum length of ten (10) characters on all systems;
ii. Not be the same as the User ID or name of the user;
iii. Not be transmitted in the clear or plaintext outside the secure location;
iv. Not be displayed when entered;
v. Not containing repeating characters;
vi. Not containing characters in sequence (e.g. 12345 or qwerty).

Multi-Factor Authentication (MFA)

- MFA, sometimes referred to as two-factor authentication or 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:
    - something you know (like a password or PIN);
    - something you have (like a smart card or physical token);
    - something you are (like your fingerprint - also known as biometrics)

- MFA will be enabled for all accounts accessing the student information system (Banner), network, servers, endpoints, or any other technology that could compromise any of those systems.
    - Students, faculty and staff will have the ability to self select their choice of receiving an MFA token (mobile app, email, SMS, or phone).
    - MFA tokens will not be required while using a device connected to the campus network.
    - MFA tokens will be required upon first sign in on any new device.

Password Protection Standards

Passwords should not be shared. All passwords should be treated as personal and confidential information.

Examples of "do not's" regarding passwords. This is not an exhaustive list and may be modified to ensure timely best practices.

- Do not reveal a password over the phone to anyone.
- Do not request someone's password.
- Do not reveal a password to a co-worker, supervisor, subordinate, or assistant.
- Do not reveal a password to a fellow student or friend.
- Do not reveal a password in electronic communication means (email, text, etc.).
- Do not talk about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- Do not share a password with family members.
- Do not write passwords down and store them anywhere in your office.
- Do not store passwords in a file on ANY computer or information system that is unencrypted.
- Do not forget to log off when using a shared computer on the college campus (e.g., public space, lab, library, classroom, etc.).

Poor, weak passwords have the following characteristics:

- The password contains less than ten (10) characters
- The password is a common and familiar words such as:

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Birthdays and other personal information such as address and phone numbers.
- Word or number patterns (e.g. aaabbb, qwerty, zyxwvuts, 123321)
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

i. If someone demands a password, refer him or her to this document or have him or her call the District Information Services office for further clarification.
ii. If an account or password is suspected to have been compromised, report the incident to your Academic Computing Departments or the District Information Services offices and immediately change all passwords.

This document was built with references to the following documentation:

1. https://www.michigan.gov/documents/msp/Password_policy_325048_7.pdf
2. https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy
3. http://www.calhoun.edu/Content/Uploads/calhouninnovate.edu/files/Calhoun_Password%20Policy.pdf
4. https://https.cio.gov/
5. https://https.cio.gov/everything/
6. https://pages.nist.gov/800-63-3/sp800-63b.html
7. https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf
8. https://www.wired.com/2016/01/you-need-a-password-manager/
9. https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication

Review History

Information Services, Information Security TCC Subcommittee: 10.8.2020
Technology Coordinating Council: 10.20.2020