Stark County Board of Developmental Disabilities

PASSWORD

POLICY

The Board recognizes that a solid password policy is perhaps the most important security control an organization can employ. Strong passwords are also a requirement for HIPAA compliance, so this policy falls in line with the Board's HIPAA policies as well. Since the responsibility for choosing good passwords falls on the users, a detailed and easy to understand policy is essential.

The purpose of this policy is to specify the Board's guidelines for use of passwords. Most importantly, this policy will help users understand why strong passwords are a necessity, and help them create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

This policy applies to any person who is provided an account on the organization's network or systems, including: employees, guests, contractors, partners, vendors, etc.

This document is part of the Board's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, the applicable policies should be reviewed as needed.

Historical Resolution Information	Reviewer(s):
Date **Resolution Number** 3/28/15 03-19-15 4/24/18 04-23-18 6/29/21 06-27-21	Information Technology Manager

Stark County Board of Developmental Disabilities

PASSWORD

PROCEDURE

I. **Construction**
   The Board mandates that users adhere to the following guidelines on password construction:

   A. Passwords should be at least 8 characters

   B. Passwords should be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)

   C. Passwords should be comprised of a mix of upper and lower case characters

   D. Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary

   E. Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)

   F. Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

II. **Confidentiality**
   Passwords should be considered confidential data and treated with the same discretion as any of the organization's proprietary information.   The following guidelines apply to the confidentiality of organization passwords:

   A. Users must not disclose their passwords to anyone

   B. Users must not share their passwords with others (co-workers, supervisors, family, etc.)

   C. Users must not write down their passwords and leave them unsecured

   D. Users must not check the "save password" box when authenticating to applications

   E. Users must not use the same password for different systems and/or accounts

   F. Users must not send passwords via email

Stark County Board of Developmental Disabilities

    G. Users must not re-use passwords

III. **Change Frequency**
In order to maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. At a minimum, users must change passwords every 90 days. The organization may use software that enforces this policy by expiring users' passwords after this time period.

IV. **Incident Reporting**
Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the IT Director. Any request for passwords over the phone or email, whether the request came from organization personnel or not, should be expediently reported. When a password is suspected to have been compromised the IT Director will request that the user, or users, change all his or her passwords.

V. **Enforcement**
This policy will be enforced by the IT Director and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of Board property (physical or intellectual) are suspected, the Board may report such activities to the applicable authorities.

Definitions

Authentication A security method used to verify the identity of a user and authorize access to a system or network.

Password A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

Two Factor Authentication A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.