MSHN
Mid-State Health Network

POLICIES AND PROCEDURE MANUAL

Chapter:	Information Technology		
Title:	Password security		
Policy: ☐ Procedure: ☒ Page: 1 of 3	Review Cycle: Biennial Author: Chief Information Officer	Adopted Date: 04.1.2023 Review Date:	Related Policies:

Purpose

The purpose of this procedure is to establish security standards, applicable to MSHN employees, for creation and protection of passwords.

Procedure

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Mid-State Health Network's (MSHN) entire corporate network, or an application that stores private/sensitive information. As such, all MSHN employees (including contractors and vendors with access to MSHN systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. Users must use "complex" passwords. that conform to the "Complex passwords" sub-section under the "General Password Construction Guidelines" shown below.

1. Users must use a unique password for each account login that they control. If they are provided a password by someone that is not unique or become aware of a password in use that is not unique, then they must take steps to correct it.
2. Passwords must never be reused. When passwords are changed, a unique (new) password must be selected and used rather than recycling a previously used password or incrementing a number in the password.
3. For Windows logins, Microsoft 365 logins, and wherever else possible, a second factor of authentication MUST be used, often referred to as multi-factor authentication (MFA) or Two-factor authentication (2FA).
4. Users are prohibited from using MSHN account passwords for any non-MSHN accounts, such as personal email, banking, social media, etc.
5. Users are prohibited from sharing passwords with anyone, even co-workers. All passwords are sensitive, confidential MSHN information.
6. Users are prohibited from inserting passwords into email messages or other forms of electronic communication, unless the message or communication is encrypted.
7. Users must change all user-level passwords (Office 365, Windows Network/Computer Login, banking sites) anytime they suspect that a password may have been compromised.
8. System Administrators must change all system-level passwords (e.g., administrator, admin, application administration accounts, etc.) anytime they suspect that a password may have been compromised.
9. Users are prohibited from storing passwords in any electronic form such as Word, Excel, Notepad, even if the file is password protected.

Chapter:	Information Technology		
Title:	Password security		
Policy: ☐ Procedure: ☒ Page: 2 of 3	Review Cycle: Biennial Author: Chief Information Officer	Adopted Date: 04.1.2023 Review Date:	Related Policies:

10. If a user suspects an account or password has been compromised, they must report the incident to the Security Officer and change the password in question immediately.
11. MSHN or a third party contractor of MSHN, may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it immediately, and may be required to take additional training. If non-compliance with this procedure continues the user may be subject to disciplinary action as indicated in the Personnel Handbook.

General Purpose Construction Guidelines

MSHN requires that workers use complex unique passwords as defined in this procedure. Below are specific guidelines for constructing these passwords.

Complex passwords have the following characteristics**:**

1. Contain both upper and lower case characters (e.g., a-z, A-Z).
2. Include digits and punctuation characters as well as letters, e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./).
3. Are at least 10 alphanumeric characters long.
4. Are not a word in any language, slang, dialect, jargon, etc.
5. Are not based on personal information, names of family, etc.
6. Are never written down or stored on-line unless within an encrypted password storage system such as LastPass.
7. Examples of complex passwords: “!Ew7q*nW49” or “A3g&n$q7V2”

Poor, weak passwords have the following characteristics and MUST be avoided:

1. They contain less than 10 characters.
2. They are a word or contain a word found in a dictionary (English or foreign).
3. Names of family, pets, friends, co-workers, fantasy characters, etc.
4. Computer terms, names, commands, sites, companies, hardware, and software.
5. The words “MSHN”, “health”, “CMH”, “mental” and geographical indicators such as “Lansing,” “Michigan” or any derivation.
6. Birthdays and other personal information such as addresses and phone numbers.
7. Word or number patterns such as aaabbb, qwerty, zyxwvuts, 123321, etc.
8. Any of the above spelled backwards.
9. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
10. The use of the word ‘Password’ in any variation with numbers.

MSHN
Mid-State Health Network

POLICIES AND PROCEDURE MANUAL

Chapter:	Information Technology		
Title:	Password security		
Policy: ☐ Procedure: ☒ Page: 3 of 3	Review Cycle: Biennial Author: Chief Information Officer	Adopted Date: 04.1.2023 Review Date:	Related Policies:

Password Protection Standards – List of Don'ts

A. Don't reveal a password to anyone over the phone.
B. Don't reveal a password in an email message.
C. Don't reveal a password to your supervisor.
D. Don't talk about a password in front of others.
E. Don't hint at the format of a password (e.g., "my family name").
F. Don't reveal a password on questionnaires or security forms.
G. Don't share a password with family members.
H. Don't reveal a password to a co-worker when you go on vacation.
I. Don't write down a password and store it anywhere in your office.
J. Don't store passwords in a file on any computer, including a handheld computer, phone, or tablet without encryption.
K. Don't use the "Remember Password" feature of any website or browser.
L. If someone demands a password, **DO NOT give it to them**.

Applies to

☒ All Mid-State Health Network Staff
☐ Selected MSHN Staff, as follows:
☐ MSHN's CMHSP Participants: ☐Policy Only ☐Policy and Procedure
☐ Other: Sub contract Providers

Definitions

Other Related Materials
N/A

References/Legal Authority
Health Insurance Portability and Accountability Act Of 1996 (HIPAA)

Change Log:

Date of Change	Description of Change	Responsible Party
4.1.2023	New Procedure	Chief Information Officer