Date: 03/28/19

Version 1.0

Password Policy Template

# 1. 0 Purpose

To provide guidance and direction to our employees about password creation, use and account management. Passwords are key to keeping your account secure and are the first line of defense to protect our sensitive company information. This policy covers both user accounts and system accounts managed by system administrators.

# 2.0 Policy - Users

A. It is our company’s policy that users shall establish and maintain strong passwords to prevent malicious actors from easily guessing the password;

B. Users are directed not to reuse passwords across multiple accounts;

C. Passwords shall be created with complexity such as pass phases, and not contain easily known or guessable elements such as names, birthdays, street addresses or sport teams;

D. Passwords shall be made up of alphanumeric (a mix of numbers and letters) with special characters such as (!@#$%^&\*()\_+) and a mix of upper and lowercase characters as guided by the software or hardware systems;

E. Passwords shall be a minimum of 8 characters long;

F. Passwords shall not be created with commonly used passwords such as Password123;

G. Passwords shall not be written down on a sticky note, displayed on public-facing screen or placed under a keyboard;

H. Passwords shall be changed periodically, as guided by the software governing the systems, using new passwords;

I. For all sensitive business accounts, two factor authentication will be enabled.

J. Passwords shall not be shared with anyone. Each employee shall have his/her own password for each account for accountability and security.

Date: 03/28/19

Version 1.0

Password Policy Template

# 3.0 Policy - Administrators

A. Limit the number of times a password can be attempted to be entered incorrectly to three or four attempts. This will prevent unauthorized individuals or programs from trying to guess passwords;

B. Set passwords to expire every 90 to 120 days;

C. Evaluate the security questions for account management. Easy-to-guess security questions (i.e. “Who was your best friend in high school?”) should not be used;

D. Any default passwords that come with a product should be changed during product installation;

E. Use screen protection to prevent someone from peeping over the employees’ shoulders;

F. Enable two factor authentication for all sensitive accounts, especially account logins used by administrators. See <https://twofactorauth.org/> for a listing of systems and services that can be enabled by two factor authentication;

G. Encourage your company’s users to utilize a password manager such as 1Password to save and manage passwords;

H. If a user account has been compromised instruct and follow through with users to ensure their password is immediately changed;

I. Encourage users to check to see if their password and login has been compromised at “I have been pwned” - <https://haveibeenpwned.com/>;

J. Instruct users that if they receive an email concerning a breach or password reset, not to click on it, but rather go directly to their account at the website.;

K. As our company’s IT security POC, leverage the educational resources provided through our account at the NCSS.

.

Password Policy Template

# 4.0 Applicability

A. This policy applies to both official company accounts and personal accounts of employees and contractors.

# 5.0 References

<https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd>

<https://pages.nist.gov/800-63-3/sp800-63b.html>

<https://www.npr.org/sections/alltechconsidered/2017/08/14/543434808/forget-tough-passwords-new-guidelines-make-it-simple>

<https://www.healthit.gov/sites/default/files/Password_Checklist.pdf>

<https://www.ibm.com/support/knowledgecenter/en/SS3JSW_5.2.0/com.ibm.help.security.doc/SI_PwdPolicies.html>

Date: 03/28/19

Version 1.0