Overview

This policy is intended to establish guidelines for effectively creating, maintaining, and protecting

passwords on information systems at ((Company Name)).

Scope

This policy shall apply to all employees, contractors, and any other person who has access to any information system at ((Company Name)). This document will also govern all acceptable password use on all internal systems that connect to ((Company Name)) network or access or store ((Company Name)) data.

Definitions

Internal Systems - A information system that is used by ((Company Name)) Employees, contractors, and vendors. These systems are not customer facing.

Policy

1. Password Creation
   1. All user and admin passwords must be at least 14 characters in length. Longer passwords and passphrases are strongly encouraged.
2. Where possible, A password manager should be utilized to prevent the use of common and easily cracked passwords.
3. Passwords must be completely unique, and not used for any other system, application, or personal account.
4. Default installation passwords must be changed immediately after installation is complete.

Password Protection

1. If passwords need to be shared, they must only be shared using an authorized method, any other means of sharing passwords is not allowed.
   1. The only exception is passwords that expire after a one time use or passwords that expire within a 24 hour period.
2. Passwords shall not be written down or physically stored anywhere in the office.
3. When configuring password “hints,” do not hint at the format of your password (e.g., “zip + middle name”)
4. User IDs and passwords must be stored in an encrypted format.
5. User IDs and passwords must not be scripted to enable automatic login.
6. “Remember Password” feature on websites and applications should not be used.
7. All PC/Macs and mobile devices that connect to the company network must be secured with a password and/or biometric authentication and must be configured to lock after 15 minutes of inactivity.

Enforcement

It is the responsibility of the end user to ensure enforcement with the policies above.

If you believe your password may have been compromised, please immediately change the password and report the incident to the company security team and your manager.