**Password Policy**

**Overview**

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to our systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

**Purpose**

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

**Scope**

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that has access to company assets, or stores any non-public company information.

**Policy**

**Password Creation**

* All user-level and system-level passwords must conform to the *Password Construction Guidelines*.
* Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.
* User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.
* All accounts should use Multi-Factor Authentication (MFA) unless technical limitations prevent doing so.

**Password Change**

* Passwords should be changed only when there is reason to believe a password has been compromised. (**Note to jobs I am applying to! This is based on recent NIST guidance and the principle that a frequently changed password is more likely to be written down / storage in an insecure manner, this policy would be different if compliance required it**)

**Password Protection**

* Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, confidential information.
* Beyond initial onboarding, passwords must not be inserted into email messages, or other forms of electronic communication, nor revealed over the phone to anyone.
* Passwords may be stored only in a user's managed 1Password vault.
* Do not use the "Remember Password" feature of applications (for example, web browsers).
* Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

**Application Development**

Application developers must ensure that their programs contain the following security precautions:

* Applications must support authentication of individual users, not generic accounts that cannot be traced.
* Applications must not store passwords in clear text or in any easily reversible form.
* Applications must not transmit passwords in clear text over the network.
* Applications must provide for some sort of role management.

**Multi-Factor Authentication**

* Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

**Policy Compliance**

**Compliance Measurement**

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

**Exceptions**

Any exception to the policy must be approved by the Infosec Team in advance.

**Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**Related Standards, Policies and Processes**

See the *Password Construction Guidelines* policy document.

* **Revision History**

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| **June 2014** | SANS Policy Team | Updated and converted to new format. |
| **July 2022** | Ivy Astrix | Initial draft. |