**Password Construction Guidelines**

**Overview**

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or networks. This guideline provides best practices for creating secure passwords.

**Purpose**

The purpose of these guidelines is to provide best practices for the created of strong passwords.

**Scope**

This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties.

**Statement of Guidelines**

Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 14 characters in your password. 1Password auto generated passwords should be used, and are in the passphrase format (ie: 'block-sunny-leaves-gear').

In addition, every work account should have a different, unique password. Each account should be stored in the users managed 1Password vault.

**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**

None.

**Definitions and Terms**

None.

**Revision History**

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