**Password Construction Guidelines**

**Last Update Status:** *Updated October 2022*

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to* [*policy-resources@sans.org*](mailto:policy-resources@sans.org)*.*

1. **Overview**

Passwords are a critical component of information security. Passwords serve to protect access to user accounts, data and systems. However, a poorly constructed or easily guessed password can compromise the strongest defenses. This guideline provides best practices for creating strong passwords.

1. **Purpose**

The purpose of this guidelines is to provide best practices for the creation of strong passwords.

1. **Scope**

This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

1. **Policy**

Strong passwords are long, the more characters a password has the stronger it is. We recommend a minimum of 16 characters in all work related passwords. In addition, we encourage the use of passphrases, passwords made up of multiple words. Examples include “*It’s time for vacation*” or “*block-curious-sunny-leaves*”. Passphrases are both easy to remember and type yet meet the strength requirements.

# Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change.

1. **Policy Compliance**
   1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to password cracking exercises, business tool reports, internal and external audits, and feedback to the policy owner.

* 1. Exceptions

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

* 1. Non-Compliance

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

1. **Related Standards, Policies and Processes**

None.

1. **Definitions and Terms**

None.

1. **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. |
| October, 2017 | SANS Policy Team | Updated to reflect changes in NIST SP800-63-3 |
| October 2022 | SANS Policy Team | Updated and converted to new format. |