SNOWBE ONLINE PSP01

Password Standard Policy

Swann Raddle
Version 1.0
05/4/25

Table of Contents

<Template Policy> – V 1.0
Status: ✠ Working Draft ☐ Approved ☐ Adopted
Document owner: Swann Raddle
DATE 05/04/25

Purpose

The purpose of the SnowBe Password Standard is to define the minimum-security requirements for the creation, use, and management of passwords across all SnowBe systems and services. This standard supports SnowBe's broader information security objectives by helping prevent unauthorized access, account compromise, and data breaches.

Scope

This standard applies to all SnowBe employees, contractors, temporary workers, vendors, and any other individuals or entities that access SnowBe information systems or services using password-based authentication.

Definitions

Authentication: The process of verifying a user's identity.
Multi-Factor Authentication (MFA): A login method requiring more than one verification method to gain access.

Passphrase: A longer string of text or words used as a password that is easier to remember but harder to guess.

Privileged Account: An account with elevated access rights, such as a system administrator.

Roles & Responsibilities

End Users: Responsible for creating strong, compliant passwords and protecting their credentials.

IT Department: Enforces password standards through system configurations and provides tools for secure password management.

Security Officer: Monitors compliance with this standard and investigate incidents related to password misuse.

Standard

General Password Requirements

- Must be a minimum of 12 characters in length.
- Must include at least three of the following four:
  - Uppercase letters (A–Z)
  - Lowercase letters (a–z)
  - Numbers (0–9)
  - Special characters (! @ # $ % ^ & * etc.)
- Must not contain dictionary words, usernames, personal info (e.g., birthdays), or sequential characters (e.g., “abcd”, “1234”).
- It should be changed every 180 days for general users.
- Privileged accounts must be updated every 90 days.

Passphrases (Recommended Option)

- May be used in place of complex passwords.
- There must be 16 characters or longer.
- Must not be based on famous quotes, lyrics, or pop culture references.

Account Lockout Policy

- After 5 failed login attempts, accounts are locked for 15 minutes.
- Repeated lockouts may lead to accountancy disablement or investigation.

Password History and Reuse

- Users may not reuse any of their previous **12 passwords**.
- Passwords must not be stored in plain text.

Password Storage and Transmission

- Passwords must be:
  - Encrypted when stored.
  - Transmitted securely over encrypted channels (e.g., TLS/SSL).
  - Hashed using strong algorithms (e.g., bcrypt, PBKDF2, Argon2).

Multi-Factor Authentication (MFA)

- Required for:
  - Remote system access.
  - Privileged accounts.
  - Access to sensitive data and regulated systems.

Password Managers

- SnowBe-approved password managers are highly recommended for generating and storing strong passwords securely.

Exceptions/Exemptions

Exceptions to this plan must be approved by the IT Director only. All exceptions will be formally documented, and you can only request an exception/exemption by contacting the IT Director and stating why the exception/exemption has been requested. A request does not mean automatic approval. Exceptions will be reviewed periodically for appropriateness. All exemptions or exceptions are temporary and are only valid for the time period allotted by the person approving it (which varies depending on circumstance); this does not affect the legitimacy of this document.

Enforcement

Failure to comply with these requirements may result in a financial penalty per incident, as well as a written report. Penalties may begin with a verbal warning, and after 3 reports, there's a potential for contract/employee termination and/or legal action.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	05/04/25	Swann Raddle	Sarah Meraz	Creating the password standard policy

Citations

Adapted from Michigan Technological University Password Standards, https://www.mtu.edu/it/security/policies-procedures-guidelines/password-standards.pdf, accessed April 28, 2025