a

SNOWBE ONLINE #004
Password Procedures

Sean Redding

Change Control Management

Policy- Version # 1.0

10-18-25

Table of Contents

Purpose

The purpose of this Procedure is to align with the Password Standard #003 for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this Procedure includes all personnel who have or are responsible for an account on any system of SnowBe Online.

Definitions

Authenticate - means verification of the identity of a user, process, or device that is requesting access to SnowBe Online's Information System.

Compromised - means an account that has been maliciously broken into and could be used by an unauthorized individual for malicious reasons.

Password Manager - means a software program that keeps a number of passwords in a secure digital location that are accessed using a single master password.

Roles & Responsibilities

The IT Director, supported by the IT Manager, is responsible for the implementation, enforcement, and revision of these Procedures.

The IT Team is responsible for managing the systems that allow employees to log in and update passwords and for ensuring that all passwords for SnowBe Online accounts meet the minimum requirements. The IT Team will notify all Snowbe Online account owners via email fifteen (15) days prior to their employee portal login password expiring.

Employees are responsible for keeping their passwords confidential and updating them regularly upon request from IT.

Procedures

- Passwords must have a minimum length of 12 characters or the maximum length the system supports if the system has a maximum password length of less than 12 characters.
- Passwords must meet at least 3 out of the 4 requirements for quality:
    - At least 1 lowercase letter
    - At least 1 upper case letter
    - At least 1 number
    - At least 1 special character. Disallowed characters are asterisk (*), percent (%), ampersand (&), and semicolon (;).
- Users must choose unique passwords that are difficult to guess. Passwords must not:
    - Contain the user's first name, middle name, last name, or username
    - Be based on a single dictionary word
    - Contain more than 2 repetitive characters (e.g., Mmmmmm1, Ab7777777, etc.)
    - Be a repeat of a password used within the last year
    - Be shared with other users
- Passwords on sensitive IT systems must be changed, at a minimum, every 90 days.
- Initial passwords must be unique and provided in a secure manner and changed upon first logon.
- After multiple unsuccessful consecutive logon attempts (e.g., incorrect passwords), the user's account may become automatically locked. Users may need to contact the Help Desk for account unlocking, or accounts may automatically unlock after a period of time
- Passwords should never be written down and left in plain sight. If a password must be written down, it should be stored in a secure location.
- Passwords should never be stored electronically in plaintext. A password manager should be used to securely store passwords electronically.
- Users must log off of applications when done using them.

- Users must secure workstations when they are away from them. Devices will be subject to lockouts for inactivity after 10 minutes.
- Users must only use their user ID and password for Snowbe Online systems and services. Users should create a different username and password for external services such as personal email, banks, online stores, personally owned computers, or other systems.
- Users must report suspected password compromises by contacting the IT Help Desk.
- Users must change their passwords if they suspect it has been compromised.

Exceptions/Exemptions

Requests for an exception must be submitted in writing to consult with the IT Director or IT Manager.

The request must be detailed with information, including:

- Length of time
- Policy or standard
- Reason

Each request will be reviewed by the IT Manager or IT Director to determine whether an exemption is justified and whether it will require compensating controls.

If the non-compliance is due to a better solution, an exception is still required and will be formally evaluated and approved.

The IT Director and the Commissioner must maintain constant communication during the exception. If approved, the Commissioner's office will send the letter of approval to the requester with details. In the event of denial, a letter of explanation will be sent to the requester with the reason the IT Director denied the request and an explanation.

Exemptions:

Access Control – Access controls, including Single Sign-On (SSO), Multi-Factor Authentication (MFA), Sessions, and IAM policies, are not to be paused or discontinued.

Enforcement

- Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director.
- Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
- Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from SnowBe.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	10-25-25	IT Director	IT Director	Initial draft of Procedure.

Citations

https://it.emory.edu/smcc/itsm_process/change/roles-responsibilities.html

https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-and-guidelines/change-control-policy/