SNOWBE ONLINE Policy PP-1

Password Procedure

POLICY

Group 2 Members:
Emma McClung

Version 2.0

DATE: 12/16/2025

Table of Contents

Purpose

A password procedure policy makes requirements for creation, usage and storage, and management of passwords clear for SnowBe password protection of information and data of unauthorized access. This helps reduce risk of credentials compromise, supports account security, and makes password practices consistent for all users, systems, and environments. Aligning security controls with organizational requirements.

Scope

This plan applies to all SnowBe employees, contractors, systems, servers, mobile devices, AWS-hosted services, retail locations, laptops using VPN, and all customer-facing platforms where password-based authentication is used.

Definitions

Information Technology (IT) Resources – Equipment or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, email, and social media sites.

Multi-factor Authentication – a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are) (Rosenblatt & Cipriani, 2013).

Roles & Responsibilities

IT Security: Implements, monitors, and reviews all access control mechanisms and privileged accounts.

System Administrators: Apply changes, manage permissions, and maintain secure configurations.

Employees: Follow assigned access privileges and report unusual access activity.

Management: Approves access requests and oversee separation of duties processes.

Policy

SnowBe requires passwords that are used to access the system, be securely created, well-managed, and protected from unauthorized access. Minimum security standards, limit reuse, prevent disclosure, and support response to compromised credentials is in the password controls and will be enforced.

Procedures

Quarterly access reviews must be performed for all privileged accounts.

Managers must approve any elevation of permissions to privileged status.

Duties involving finance, customer data, and system administration must be segregated.

Privileged actions must be logged and monitored for anomalies.

Passwords must be kept confidential and must not be shared.
Passwords must meet minimum length and complexity requirements.
Password reused shall be limited.
Passwords must not be stored in plain text or written down.
Default passwords must be changed immediately upon first use.
Passwords must be changed if system security is suspected to be compromised.
Passwords must not be hard coded into software or stored in scripts, logs, browsers, or communication utilities unless encrypted.
Temporary or reset passwords must be changed upon first use.
Passwords must be periodically reviewed for compliance where technical capability exists.

Exceptions/Exemptions

Exceptions to, or exemptions from, any provisions of the Security Plan and/or supplemental policies, standards, or guidelines must be approved by SnowBe's Information Technology Manager or higher. Any questions about the contents of this plan and/or supplemental policies, standards, or guidelines should be referred directly to the Information Technology Manager or a member of the department who has the responsibility to interpret the security standard. Please submit the following:

- A written document with reasoning
- Length of exemption/exception (cannot be longer than 30 days).
- Signed by the requester
- Signed by the requester's manager
- Signed by the requester's department head

Enforcement

All SnowBe employees, including the CEO, CFO, CIO, CTO, as well as remote employees, temporary employees, volunteers, guests, contractors, agents, and any third parties acting on behalf of SnowBe, are required to comply with SnowBe policies, standards, and guidelines. Should you be found in violation, you may be subject to the following disciplinary actions:

- Verbal warning
- Write-up
- Meeting with IT Manager/Mandatory Training
- Termination and/or legal action

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1	12/1/25	Group 2 members	Group 2 Leader	Entered clause for Exceptions/Exemptions
2	12/16/25	Group 2 members	Emma McClung	Updated with PP-1 policie.

Citations

New York State Education Department. (2019). *NYSED ISO Policy: User Account Password Policy*. https://www.nysed.gov/sites/default/files/programs/data-privacy-security/nysed_secp5-v3_useraccountpasswordpolicy.pdf (Definitions)

Southern University Baton Rouge (SUBR). (2007). *PASSWORD POLICY* [Policy]. https://www.subr.edu/assets/subr/DoIT/Password-Policy-April-2019.pdf (policies & procedures)

OpenAI. (2025). *ChatGPT* (GPT-5.2) [Large language model]. https://chat.openai.com/

(polishing language)