SNOWBE ONLINE
PSWP#1 PASSWORD PROCEDURE

Your name:
Christopher Stevens

PASSWORD PROCEDURE

Version # 1.0

DATE: 6-1-2025

PASSWORD PROCEDURE – V 1.0
Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document owner: Chris Stevens
DATE: 6-1-2025

Table of Contents

Purpose

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. The purpose of this Procedure is to establish a standard for 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 (or any form of access that supports or requires a password) on any system that resides at any SnowBe Online facility, has access to the SnowBe network, or stores any non-public SnowBe information.

Definitions

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

Brute Force Attacks
Trial-and-error method used to obtain desired information such as user passwords.

Compromised
An account that has been maliciously broken into and could be used by an unauthorized individual for nefarious reasons.

Organizational Users
An employee, students, or individual the Company deems to have equivalent status of an employee or student including, but not limited to, contractors, guest researchers, and individuals from another organization or University.

Password Vault
A software program that keeps a number of passwords in a secure digital location that are accessed using a single master password. Also called Password Manager (e.g., LastPass).

Privileged Access Manager
A tool that provides secure privileged access to critical assets (e.g., BeyondTrust).

Service Account
Is an identity that is tied to a system service or function within an information system. Although it may be controlled by an individual, the individual may not be interactively present when the service account is used by the system. This is normally used as part of automated processes between applications or systems and does not require interactivity on the part of an individual.

User Account
Is an identity that is directly tied to an individual and is used in the performance of that individual's work role or job function. This may include user accounts with elevated privileges. This also includes accounts used by people outside of SnowBe Online (such as contractors or vendors), whenever those accounts are used to access SnowBe Online systems.

Roles & Responsibilities

Chief Information Officer ("CIO"),

Chief Information Security Officer ("CISO")
Is responsible for implementation and enforcement of this Standard.

Identity and Access Management ("IAM")
Is responsible for managing the systems that allow Organizational Users to claim their SnowBe Online Account and update passwords and for ensuring that all passwords for SnowBe Accounts meet the minimum requirements. IAM will notify all SnowBe Online Account Owners via email fifteen (15) days prior to their Login password expiring.

Authorizing Official
Approves or denies account requests, ensuring alignment with business and security requirements. Typically, the IT Manager or department head.

Human Resources (HR)
Initiates account requests for new employees and notifies IT of terminations to deactivate accounts.

IT Administrator
Creates, configures, and disables accounts, ensuring compliance with security settings (e.g., encryption, password policies).

Requestor
An employee, contractor, or vendor submitting a new account request, providing justification and required details.

Security Officer
Reviews account requests for compliance with PCI standards and security policies, ensuring least privilege.

Procedure

Passwords are used for various purposes at SnowBe Online. Some of the more common uses include user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

1. The password contains less than ten characters

2. The password is a word found in a dictionary (English or foreign)

3. The password is a common usage word such as:
    a. Names of family, pets, friends, co-workers, fantasy characters, etc.
    b. Computer terms and names, commands, sites, companies, hardware, software.
    c. Birthdays and other personal information such as addresses and phone numbers.
    d. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    e. Any of the above spelled backwards.
    f. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

1. Contain both upper- and lower-case characters (e.g., a-z, A-Z)

2. Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:”;’<>?,./)

3. Are at least ten alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).

4. Are not a word in any language, slang, dialect, jargon, etc.

5. Are not based on personal information, names of family, etc.

6. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: “This May Be One Way To Remember” and the password could be: “TmB1w2R!” or “Tmb1W>r~” or some other variation.

NOTE: Do not use either of these examples as passwords!

Password Protection Standards

Generally, do not use the same password for SnowBe Online accounts as for other non-SnowBe access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, do not use the same password for various SnowBe Online access needs. For example, select one password for the Engineering systems and a separate password for IT (Information Technology) systems. Also, select a separate password to be used for a Windows account and a UNIX account. Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.

Here is a list of "don’ts":

- Don't reveal a password over the phone to ANYONE

- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don’t store your password anywhere on your desk
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them contact the SnowBe Online IT Service Desk.

Do not use the "Remember Password" feature of browsers or applications (e.g., Internet Browser, Outlook, Gmail, Hotmail).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including mobile devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to the IT Service Desk and change all passwords.

Exceptions/Exemptions

Exceptions to this plan must be approved by the Information Security Office, under the guidance of SnowBe's IT Director and/or IT Manager. All exceptions will be formally documented. Plan exceptions will be reviewed on a periodic basis for appropriateness. Please note that while requesting exceptions or exemptions has been made available to you, it does not guarantee approval.

SnowBe Online recognizes that, under certain circumstances, deviations from this Acceptable Use Policy may be necessary to support specific business needs or technical requirements. Exceptions or exemptions to this policy may be granted under the following conditions:

Risk Acceptance
In some rare cases, a business case for non-compliance can be established. In all such cases, the non-compliance situation must be approved in advance through a risk acceptance process. This process requires a risk acceptance memo signed by a department manager and reviewed by IT Enterprise Security and IT Information Systems and approved by the IT Director and/or IT Management. Further details on the risk acceptance process can be obtained through the Enterprise IT Security Department.

Pre-Approval Required
All exceptions must be formally requested in writing and approved by the IT department and an authorized member of management. The request must clearly state the business justification, duration, and potential risks of the exception.

Documentation and Review
Approved exceptions will be documented and maintained by the IT department. All exceptions are subject to periodic review to ensure they remain valid and do not introduce unacceptable risks.

Temporary and Specific
Exceptions are granted on a temporary basis for clearly defined scopes and timeframes. They do not constitute a permanent change to the policy.

No Unauthorized Exceptions
Any deviation from this policy without documented approval is considered a violation and may result in disciplinary action, including suspension of access privileges.

Compliance Priority
Exceptions will not be approved if they compromise SnowBe Online's compliance with legal, regulatory, or security requirements.

Enforcement

Enforcement
SnowBe Online takes the enforcement of this (Policy name) seriously to protect its systems, data, and customers.

Violations of this policy, whether intentional or accidental, may result in disciplinary action, up to and including termination of employment, contract cancellation, and/or legal action.

The penalties will include the following components:

Monitoring and Auditing
SnowBe Online reserves the right to monitor, log, and audit all system and network activity to ensure compliance with this policy. Users should have no expectation of privacy when using company-owned systems or accessing company data.

Incident Investigation
Suspected policy violations will be investigated promptly by the IT department, Human Resources, and other relevant stakeholders. Users are expected to cooperate fully during any investigation.

Corrective Action
If a violation is confirmed, corrective actions will be taken based on the severity and nature of the breach. This may include revocation of access, mandatory training, written warnings, or other disciplinary measures as outlined in the employee handbook.

Legal Consequences
Activities that are illegal under local, state, or federal law may be reported to the appropriate authorities. This includes unauthorized access, data breaches, or misuse of customer financial information.

Appeals Process
Individuals who believe they were unfairly penalized for a policy violation may appeal the decision to management or HR following internal dispute resolution procedures.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	6-1-2025	Chris Stevens	IT Management	PASSWORD PROCEDURE Creation for use by SnowBe Online.

Citations

Bowie State University
https://www.bowiestate.edu/files/resources/information-security-public.pdf
Exceptions/Exemptions

ChatGPT
https://chatgpt.com/c/681bc793-d1dc-800b-a676-cb7b3cf2678d
Exceptions/Exemptions, but as a group we revised the verbiage.

Policy Template
https://www.sans.org/information-security-policy/
Exceptions/Exemptions

Rock Valley College
https://rockvalleycollege.edu/_resources/files/procedures/2-30-060-Procedure-Passwords.pdf
Purpose, Scope, Procedure

Alabama Community College System
https://info.accs.edu/default/assets/file/B_PasswordPolicy.pdf
Used for example formatting, Verbiage