SNOWBE ONLINE

PSWS#1

PASSWORD STANDARD

Your name:
Christopher Stevens

PASSWORD STANDARD

Version # 1.0

DATE: 6-1-2025

Table of Contents

Purpose

The purpose of this Standard is to establish the minimum requirements for passwords used to access University Information Systems to reduce the risk of Unauthorized Access to University technology resources and data.

Scope

This Password Standard applies to all SnowBe Online employees, contractors, and third-party vendors who are provisioned with or interact with any user accounts or credentials for accessing SnowBe Online's IT systems, applications, and data. This includes, but is not limited to, accounts for the AWS platform, on-premises servers, desktops, laptops, network devices, and all applications such as customer relationship management (CRM) and order management systems. The standard covers all passwords, passphrases, and other authentication credentials used for accessing or managing SnowBe Online's resources, regardless of whether the access is internal or external, or the data being accessed is company-owned, customer data, or payment card 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.

Standard

Passwords used for all SnowBe Online Accounts must be strong, preferably passphrases that are at least 12 characters long or randomly generated passwords.

1. Passwords for all Login Accounts must never include the following:
    - Three (3) consecutive characters from the first name, middle name, last name or

username.
- Blank spaces.
- Special character sequences such as //.
- Personal or financial information such as Social Security or credit card numbers.

2. Pursuant to the Acceptable Use of Data and Technology Resources, passwords must never be left in a location, along with the username, that can be readily obtained and utilized by another individual to Authenticate to a Information System.

3. To prevent compromise of Credentials, never use the same password for multiple Accounts and/or personal accounts. This includes using same password for the same account in separate instances (e.g., dev, test, prod) of a Information System or the same password for multiple accounts across the same instance.

4. Never share a password with anyone in any way (e.g., email, phone call, electronically via the Internet) including managers, co-workers, assistants, family members, friends, or the ITS/HSCITS Help Desk.

5. A password to any SnowBe Online Account is suspected to have been Compromised, it must be changed immediately, and the incident reported to Information Technology Services.

6. Use of default passwords for Administrative Accounts is prohibited.

7. Login Credentials must be used for Authentication. Local accounts should only be used for Authentication when use of EDS is technically not possible.

8. SnowBe Online Information Systems must automatically lock after no more than eight (8) unsuccessful, consecutive logon attempts to deter Brute Force Attacks.

9. Avoid storing Login and Personal Administrative Account credentials in SnowBe Online Information Systems not meant to store passwords.

10. Do not store personal account credentials (e.g., utility account, bank account) in the SnowBe's password management tools (e.g., BeyondTrust, LastPass).

11. SnowBe Online's Information Systems must support unique user accounts and passwords so that individuals do not share a username and/or password to access an application unless using a Shared Application Account.

12. Passwords must never be stored electronically in plain text such as in a document, spreadsheet, or .txt file.

13. Passwords must be protected in transit using industry-standard cryptographic protections.

14. Passwords must be hidden by default during login process.

15. Users are prohibited from re-using the last five (5) passwords previously used and the same password must not be reused within a year.

16. Temporary passwords must be set to change upon first logon.

17. Uniform responses must be provided for failed login attempts. Simple error messages such as “Access Denied” should display for a limited time before obscuring it.

18. Failed attempts must be logged unless such action results in the display of the failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect logs and report any irregularities or compromises to Information Technology Services.

19. Log files must never contain password information.

20. Passwords of Compromised accounts must be reset in a timely manner or require users to reset their own passwords in situations where continued use of a password creates risk of unauthorized access to the computing account or resource.

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	Creation of Password Standard Policy for SnowBe Online use.

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

West Virginia University
https://it.wvu.edu/policies-and-procedures/acceptable-use/password-standard
Purpose, Scope, Responsibilities, Standards