SNOWBE ONLINE Policy# SOP-PS-1

Password Standard Policy

Humberto Gonzalez

Password Standard

Version # 4.0

DATE: July 27, 2024

Table of Contents

PURPOSE 2

SCOPE 2

DEFINITIONS 2

ROLES & RESPONSIBILITIES 2

STANDARD 3

EXCEPTIONS/EXEMPTIONS 5

ENFORCEMENT 6

VERSION HISTORY TABLE 6

CITATIONS 7

Purpose

This Password Standard aims to provide a solid foundation for establishing, maintaining, and managing passwords for SnowBe Online. This standard requires that all passwords used within the business have a minimum level of complexity and security, protecting critical information and systems from unauthorized access. The standard aligns with industry best practices and regulatory standards, including NIST, PCI DSS, and other related guidelines.

Scope

This Password Standard applies to all SnowBe Online employees, contractors, and third-party users who utilize SnowBe Online systems, networks, and applications. It applies to all accounts that require password authentication and any system that supports Multi-Factor Authentication (MFA).

Definitions

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

Hashing: The process of converting a password into a fixed-size string of characters, which is typically a hash code.

Multi-Factor Authentication (MFA): An authentication system or an authenticator that requires more than one authentication factor for successful authentication.

Passphrase: A sequence of words or other text used to control access to a computer system, program, or data.

Peppering: Adding a secret value to a password before hashing, which is known only to the system and not to users.

Salting: Adding random data to a password before hashing to ensure that identical passwords generate different hash codes.

Roles & Responsibilities

Employees: Must comply with the password standard regulations and report any suspicious activity or violations related to password security.

IT Department: Responsible for managing the technical parts of the password standard, including implementation, maintenance, and documentation of password policies and MFA configurations.

Responsibilities of Systems Processing Passwords:

All SnowBe Online systems—including, but not limited to, servers, applications, and websites hosted by or for SnowBe Online—must be designed to accept passwords and transmit them with proper safeguards.

Passwords should be prohibited from being displayed when entered, although a method to toggle visibility as needed is acceptable.

Passwords must never be stored in clear, readable format. Reasonably strong, brute-force-resistant hashing methods or encryption must always be used.

Hashing, including salting and peppering (if possible), should be used instead of encryption.

Hashed or encrypted passwords must never be accessible to unauthorized individuals.

Passwords must never be stored as part of a login script, program, or automated process.

Where any of the above items are not supported, a variance request should be submitted to the IT Department for review. Appropriate authorizations and access control methods must be implemented to ensure only a limited number of authorized individuals have access to passwords.

Senior Management/Executive Team: Sets the tone and direction for password security, and allocates resources to manage password security successfully.

Third-Party Vendors: Must comply with SnowBe Online's password standards and ensure that their access is limited to only the resources required for their job. Access concerns or breaches must be reported immediately.

Standard

1. **Password Creation**

General Users:

Must be at least 12 characters in length.

Uppercase and lowercase letters, numerals, and special characters must all be present.

Must not contain easily guessable information such as usernames, birthdates, or common words.

Privileged Users (e.g., Administrators, Managers):

Must be at least 16 characters in length.

Uppercase and lowercase letters, numerals, and special characters must all be present.

Must use passphrases where feasible.

Must not be reused for at least ten previous passwords.

Must use a different password for each system or application they access.

2. **Password Management**

General Users:

Passwords must be changed every 90 days.

Users must not share passwords with others.

Users must store passwords securely and not write them down or store them in plain text.

Users must undergo regular security training and awareness programs

Privileged Users (e.g., Administrators, Managers):

Passwords must be changed every 60 days.

Users must use a password manager to generate and store complex passwords.

Users must not share passwords with others.

Users must store passwords securely and not write them down or store them in plain text.

Users must use different passwords for each privileged account they hold.

Users must undergo regular security training and awareness programs.

3. **Multi-Factor Authentication (MFA)**

MFA must be enabled for all accounts with access to sensitive information or critical systems.

Acceptable MFA methods include:

Hardware tokens (e.g., YubiKey)

Software tokens (e.g., Google Authenticator, Microsoft Authenticator)

Biometric authentication (e.g., fingerprint, facial recognition)

SMS or email verification as a secondary method (Note: SMS/email should be used only when other methods are not feasible due to potential vulnerabilities).

4. **Account Lockout**

   Accounts will be locked after five unsuccessful login attempts. The lockout duration is 30 minutes.

5. **Password Reset**

   Password reset requests must be verified through MFA, ensuring the use of a secondary method of authentication, such as a hardware token, software token, or biometric authentication.

6. **Monitoring and Auditing**

   Privileged accounts will be monitored continuously for suspicious activity.

   Regular audits will be conducted to ensure compliance with the password standard.

   Any anomalies or breaches must be reported immediately to the IT and Security teams.

7. **Password Storage for Privileged Users**

   Privileged users must use a secure password manager approved by the IT department to store and manage passwords.

   The password manager must support strong encryption to protect stored passwords.

   Access to the password manager must be protected by MFA.

Exceptions/Exemptions

In circumstances where regular security standards cannot be followed, exceptions or exemptions may be requested. To request an exception or exemption, the requester must send a formal written request to the IT department, outlining the precise security protocol that cannot be followed and the justification for the request. The request should include a reason for why the exception or exemption is required, the potential impact on security, and any proposed compensatory controls. The Chief Information Officer (CIO) or a designated senior IT executive has the power to approve or reject such requests. Approved exceptions or prohibitions will be provided for a brief period not exceeding one year unless otherwise justified. The requester must make certain that the exception or exemption is reviewed and re-evaluated before the end of the permitted term.

Enforcement

All SnowBe Online employees, contractors, and third-party entities must comply with this security policy. Failure to follow the policies and procedures outlined will result in disciplinary action, which may include verbal or written warnings for minor infractions, temporary suspension from duty for repeated or serious violations, and termination of employment for severe or repeated noncompliance. If noncompliance results in legal consequences or financial loss for SnowBe Online, the company has the right to take legal action. Contractors and third-party entities that violate this security strategy may face contract termination and legal action, depending on the severity of the breach. All disciplinary actions will be carried out under SnowBe Online policy and any applicable labor laws. Each individual must understand and follow security policies to protect the company's information assets.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
4.0	07/27/2024	Humberto Gonzalez	Robin Groff Alarcon	Password Standard Policy Implemented.

Citations

Definitions- Security and Privacy Controls for Information Systems and Organizations (nist.gov) | End of support for IBM QRadar Network Security 5.5.0

Enforcement- Sample Detailed Security Policy (bowiestate.edu)

Exceptions/Exemptions- Sample Detailed Security Policy (bowiestate.edu)

Password Standard- 11.15 - Password Policy | Information Technologies & Services (cornell.edu)