SNOWBE ONLINE Policy# SOP-PP-1

Password Procedure

Humberto Gonzalez

Password Procedure

Version # 4.0

DATE: July 27, 2024

Table of Contents

Purpose

The purpose of this password procedure is to give simple instructions for setting up, updating, and controlling passwords in SnowBe Online. By following this process, all passwords used within the company are guaranteed to adhere to the Password Standard and enhance the overall security of SnowBe Online's data and systems.

Scope

This Password Procedure 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.

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.

Roles & Responsibilities

Employees: Follow the password procedure. Report any unusual behavior or security issues.

IT Department: Implement and support the password procedure, help users, and monitor compliance.

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: Provide resources, and ensure compliance with password security.

Third-Party Vendors: Must comply with SnowBe Online's password protocols and report any security issues immediately.

Procedure

1. **Creating a Password**

For All Users:

1. Log into your SnowBe Online account.
2. Go to "Account Settings" or "Security Settings."
3. Choose the option to change or create a new password.
4. Create a password that is at least 12 characters long, using a mix of:
    - Uppercase letters (A-Z)
    - Lowercase letters (a-z)
    - Numbers (0-9)
    - Special characters (!, @, #, etc.)
5. Confirm the new password by typing it again.
6. Save the changes.

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

1. Follow the steps above.
2. Make sure the password is at least 16 characters long.
3. Use a password manager to create and store your passwords.
4. Use a different password for each system or application.

2. Using Multi-Factor Authentication (MFA):

Setup MFA for Your Account:

1. Log into your SnowBe Online account.
2. Go to "Account Settings" or "Security Settings."
3. Find the section labeled "Multi-Factor Authentication (MFA)" and select "Set up MFA."
4. Choose your preferred MFA method from the available options:

   Hardware Token:

   1. Select "Hardware Token."
   2. Follow the on-screen instructions to register your hardware token (e.g., YubiKey).
   3. Insert the hardware token into your computer’s USB port when prompted and press the button on the token.

   Software Token:

   1. Select "Software Token."
   2. Download and install an authenticator app on your smartphone (e.g., Google Authenticator, Microsoft Authenticator).
   3. Open the authenticator app and scan the QR code displayed on the screen or enter the setup key manually.
   4. Enter the code generated by the authenticator app into the SnowBe Online setup page.

   Biometric Authentication:

   1. Select "Biometric Authentication."
   2. Follow the on-screen instructions to register your biometric data (e.g., fingerprint, facial recognition) using your device’s built-in sensors.

   SMS or Email Verification:

   1. Select "SMS Verification" or "Email Verification."
   2. Enter your mobile phone number or email address.

    3. You will receive a verification code via SMS or email. Enter this code on the SnowBe Online setup page.

5. Complete the setup by following any additional on-screen instructions.
6. Verify that MFA is active by logging out and logging back into your account. You should be prompted to enter your password and then complete the second step of verification using the chosen MFA method.

3. **Managing Your Password:**

For All Users:

1. Change your password every 90 days.
2. Never share your password with anyone.
3. Use a password manager to store your passwords securely.

For Privileged Users:

1. Change your password every 60 days.
2. Use a different password for each privileged account.
3. Undergo regular security training sessions.

4. **Account Lockout:**

1. Your account will be locked for thirty minutes if your password is entered incorrectly five times.
2. Contact the IT Department if you need help unlocking your account.

5. **Resetting Your Password:**

If you forget your password:

1. Go to the login page and click "Forgot Password."
2. Follow the instructions to verify your identity using MFA.
3. Create a new password following the steps above.
4. Confirm and save the new password.

6. **Monitoring and Auditing:**

   The IT Department will monitor privileged accounts for unusual activity.

   Regular checks will be conducted to ensure everyone follows this procedure.

   Report any security concerns to the IT or Security teams immediately.

7. **Password Storage for Privileged Users:**

   Use a secure password manager approved by the IT Department.

   Ensure the password manager supports strong encryption.

   Protect access to the password manager with 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 Procedure Implemented.

Citations

Definitions- Security and Privacy Controls for Information Systems and Organizations (nist.gov)

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)