SNOWBE ONLINE Procedure# AP-3 Password Procedure

Michael Kohronas:

<Password Procedure>

Version #3

DATE: 06/2024

<Password Procedure> – V 3.0
Status: ✠ Working Draft ☐ Approved ☐ Adopted
Document owner: Michael Kohronas
DATE – 06/2024

Table of Contents

Procedure

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 facility, has access to the SnowBe network, or stores any non-public SnowBe information.

Definitions

Elevated Privileges – Privileges that are given to an account that are higher than what a normal user accounts permission would entail within the SnowBe environment.

Passphrases – A type of way to write passwords that involve writing a phrase rather than a mess of numbers and letters. This will allow for longer passwords which are easier to remember

Password Cracking Test – A security measure deployed by SnowBe that brute forces a set of passwords within SnowBe to test the strength of the passwords. This will help mitigate potential vulnerabilities by testing SnowBe users passwords.

“Remember Password” Feature – This feature permanently keeps you logged in which could allow unauthorized access within SnowBe.

One Time Pin (OTP) – A code that is sent to a device used commonly for 2 factor authentication

Roles & Responsibilities

All Employees, contractors, or interns – All employees, contractors, and contractors are required to follow SnowBe’s password Procedure and ensure that their password meets the minimum-security requirements of this Procedure.

CISO – Oversees and ensures that the password Procedure that was created covers all guidelines are covered to create a environment with strong password protection.

IT Help Desk – Manages password reset requests.

IT Security team – Monitors and ensures that all employees are following the Password Procedure and that there aren’t any duplicates by comparing hashes and reaching out to any employee, contractor, or intern if there is any issues with how they are handling their password.

Procedure

1. Password Creation:

1. Initiate the password creation process:
    - Begin by accessing the SnowBe secure password creation & management portal.
2. Choose a strong password or Passphrase
    - Select a strong set of letters and numbers to secure your account. SnowBe recommends the use of passphrases to be able to simply remember your password.
3. Ensure your password follows password standard
    - Double check your password and ensure it complies with the Password standard.
    - Ensure the passwords uniqueness and that there aren't any common words or phrases used or can relate exactly to you (e.g. pet name, family name, favorite sports team, etc)
4. Confirm Password
    - Re-enter your password into the confirmation field
5. Submission
    - Success: Click the "create password" button below the confirmation field to be redirected to a success page
    - Failure: view the reason why the password failed and ensure that it meets requirements listed in the password standard document.

2. Password Events:

1. Regular Password Reset
    - The password reset process is initiated every 6 months to 1 year (refer to password standard to see how long until your account type gets prompted).
    - A prompt password reset prompt will appear the next login attempt after the process was initiated.
    - Follow steps 2 to 5 in the "Password Creation" section of this document.
2. Change Password/Forgot Password
    - To initiate the password change process, call into the SnowBe help desk and provide the One Time Pin (OTP) to confirm the employee's identity.
    - Locate the email sent by the IT help desk and repeat it back to them.
        - The next time the user tries to login a prompt to reset password will be required.
        - If the password was forgotten a temporary password will be provided for next login.
3. Compromised password
    - If your password is compromised immediately change your password and contact the IT Help Desk team which will escalate it to the security team after assessing the situation.
        - Help Desk team will ask a list of premade questions and create a ticket for the Security team to view
        - You will hear back from the SnowBe security team the same day or the following depending on the severity of the case.

Exceptions/Exemptions

Exceptions to this Procedure will be considered on a case-by-case basis and do not guarantee approval. To request an exception, please submit a written request to the IT Director outlining the following:

How to Request Exceptions/Exemptions?
To request an Exception or Exemption from a Procedure that is in place please message ITDirector@SnowBe.com with the following format:

What Exception/Exemption are you requesting?

Why are you requesting this Exception?

How long are you requesting this Exception/Exemption for?

The IT Director, in consultation with relevant stakeholders, will review the request and determine if an exception can be granted. The decision will be based on the potential impact on security, the justification provided, and the availability of alternative secure solutions. Exceptions/Exemptions are subject to change at any point in time to strengthen security posture

Enforcement

The failure to comply with policies, Procedures, or Procedures will result in a warning or disciplinary action depending on the severity of the infraction.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
v1	06/06/2024	Michael Kohronas		Added the exception and exemption and enforcement as a group
V2	06/07/2024	Michael Kohronas		Fixed issues with text size and font, added name and date to header,
V3	06/24/2024	Michael Kohronas		Added Password Procedure Information

Citations

https://resources.finalsite.net/files/v1643750216/sdcoenet/zr6fm9smf8smkd13krit/TemplatePasswordProcedure.docx
https://info.accs.edu/default/assets/file/B_PasswordPolicy.pdf