SNOWBE ONLINE PROCEDURE PP-1
PASSWORD PROCEDURE

Ydali Hernandez

Password Procedure-1 -1.0

July 26, 2024

Table of Contents

Purpose

Passwords are a crucial aspect of computer security, serving as the frontline defense for user accounts. The purpose of this procedure is to establish a standard for creating strong passwords, protecting them, and changing them regularly to enhance the security of SnowBe Online's systems and data.

Scope

This procedure applies to all personnel at SnowBe Online who have or are responsible for an account (or any form of access that supports or requires a password) on any system residing at any SnowBe facility, accessing the SnowBe network, or storing any non-public SnowBe information.

Definitions

System-Level Passwords:
Passwords for accounts with access to system-wide settings and functionalities (e.g., root, enable, application administration accounts).
User-Level Passwords:
Passwords for individual user accounts used for everyday access (e.g., email, web, desktop computer).

Roles & Responsibilities

Director of Information Technology:
- Maintain and update the Password Protection Standards.
- Ensure password update reminders are sent to users.

Users:
- Adhere to the password creation and protection guidelines.
- Report any suspected password compromise to the IT department immediately.

Procedure

Password Creation

1. **Accessing the Password Management System:**
    a. Navigate to the SnowBe Online intranet portal.
    b. Click on the "Password Management" link.
2. **Creating a New Password:**
    a. Enter your current username and temporary password provided by IT.
    b. Follow the prompts to create a new password.
    c. Ensure the new password meets the following standards:
        i. Minimum of 12 characters.
        ii. Must include at least one uppercase letter, one lowercase letter, one

number, and one special character (e.g., !, @, #, $).
   d. Confirm the new password by entering it again.
3. **Completion:**
   a. Once the new password is confirmed, click “submit”.
   b. A confirmation message will be displayed, and the new password will be active immediately.

Password Change

1. **Periodic Change Notification:**
   a. Users will receive an email notification 10 days before their password expires.
2. **Changing the Password:**
   a. Navigate to the SnowBe Online intranet portal.
   b. Click on the “Password Management” link and log in with your current credentials.
   c. Select “Change Password”.
   d. Enter your current password.
   e. Enter and confirm the new password following the standards mentioned above.
   f. Click “Submit”.
3. **Verification:**
   a. A confirmation message will be displayed indicating the password change was successful.

Password Recovery

1. **Forgotten Password:**
   a. Navigate to the SnowBe Online login page.
   b. Click on the “Forgot Password” link.
   c. Enter your username and follow the prompts to verify your identity using multi-factor authentication (MFA).
   d. An email with a password reset link will be sent to your registered email address.
2. **Resetting the Password:**
   a. Click on the password reset link in the email.
   b. Enter and confirm a new password following the standards mentioned above.
   c. Click “Submit”.
3. **Completion:**
   a. A confirmation message will be displayed, and the new password will be active immediately.

Exceptions/Exemptions

To request an exception or exemption, the individual must submit their request to the department manager, who then will forward it to the IT department manager. The request must include a detailed explanation of the necessity for the exception or exemption, covering the business or technical reasons that justify the deviation from the standard policy.
The IT Manager will review the request to ensure all required information is provided and will assess the potential security impact. A formal risk assessment will be conducted to evaluate the implications

of the requested exception or exemption.
The IT Manager will then either approve or deny the request. The duration for the exception or exemption will be 18 months unless the requester specifies otherwise. Additionally, the exception or exemption will be subject to periodic reviews to ensure it remains necessary and that security risks are adequately managed.

Enforcement

Violations to this policy will result in disciplinary actions.

- 1st offense: Write up
- 2nd offense: Write up and training courses
- 3rd offense: Write up and leave without Pay
- 4th offense: Termination

Devices that do not comply with the security policy will be disconnected from the network until compliance is achieved.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1	07/26/24	Ydali Hernandez	R. Alarcon	Initial procedure draft

Citations

(n.d.). *Password Procedure*. Rock Valley College. Retrieved July 26, 2024, from https://rockvalleycollege.edu/_resources/files/procedures/2-30-060-Procedure-Passwords.pdf

AVP Information Technology (2011, October 28). *UB Network Connection Policy*. University at Buffalo. Retrieved July 5, 2024, from https://www.buffalo.edu/administrative-services/policy1/ub-policy-lib/ub-network-connection.html

Michigan Tech (2011, October 13). *Information Security Plan*. Michigan Technological University. Retrieved July 5, 2024, from https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-plan.pdf

University of Colorado (n.d.). *IT Security Program*. Retrieved July 5, 2024, from https://www.cu.edu/ope/aps/6005