SNOWBE ONLINE

Procedure # PP-01

Password Procedure

Daphnie Bruno

Procedure # PP-01 Version # 1.1

November 20, 2024

Table of Contents

Purpose

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 requires a password) on any system that resides at any SnowBe Online facilities, has access to the SnowBe Online network, or stores any non-public SnowBe Online information on premise or in the cloud. Employees, contractors and temporary staff must follow all SnowBe Online password procedures.

Definitions

This section provides essential definitions for key terms used throughout the password procedure, ensuring clarity and consistent interpretation of the guidelines and requirements outlined for SnowBe Online.

Authentication:
The process of verifying the identity of a user or system.

Cleartext:
Unencrypted data that can be read without any special measures.

Complexity:
The state of being intricate or complicated.

Composed:
Made up of various parts or elements.

Compromised:
Having been exposed to risk or danger, especially in terms of security.

Confidential:
Intended to be kept secret or private.

Conform:
To comply with rules, standards, or laws.

Delegates:
People authorized to act on behalf of others.

Elevated:
Raised to a higher level, often referring to increased privileges or access.

Encryption:
The process of converting information into a code to prevent unauthorized access.

Expiration:
The end of a period of validity or effectiveness.

Exploitation:
The act of using something in a way that may be considered unfair or unethical.

Functionality:
The range of operations or features that can be performed by a system.

Multi-Factor:
Involving two or more different elements or features.

Passphrases:
A sequence of words used for authentication, typically longer than a password.

Precautions:
Actions taken to prevent something dangerous or unpleasant from happening.

Privileges:
Special rights or advantages granted to certain individuals or groups.

Questionnaires:
Lists of questions used to gather information from respondents.

Verification:
The process of establishing the truth, accuracy, or validity of something.

Roles & Responsibilities

This section outlines the specific duties and accountabilities of various roles within our organization regarding the implementation, management, and enforcement of password procedures. Clear delineation of responsibilities ensures effective password security practices and promotes a culture of cybersecurity awareness across all levels of the company.

Chief Information Security Officer (CISO)

- Oversee the development and implementation of the organization's password policy
- Ensure alignment of password procedures with overall information security strategy
- Approve major changes to password requirements and procedures
- Review and assess the effectiveness of password policies periodically

Compliance Officer

- Ensure password procedures comply with relevant regulations and industry standards
- Conduct regular audits to verify adherence to password policies
- Report compliance issues related to password management to the CISO
- Assist in updating password procedures to meet new compliance requirements

Customer Service

- Assist users with password-related issues while adhering to security protocols
- Guide customers through secure password reset processes
- Educate customers on password best practices during interactions

Employees

- Create and maintain strong, unique passwords for all accounts
- Adhere to the organization's password policy and procedures
- Report any suspected password compromises or security incidents
- Participate in regular password security training

Human Resources

- Incorporate password policy training into new employee onboarding processes
- Coordinate with IT to ensure proper account creation and deletion for employees
- Assist in enforcing disciplinary actions for password policy violations

IT Security Manager

- Develop and maintain detailed password management procedures
- Oversee the implementation of password management tools and systems
- Coordinate password-related security initiatives across IT teams
- Report on password policy effectiveness to the CISO

IT Security Officer

- Monitor password-related security events and incidents
- Conduct regular password strength audits and assessments
- Implement and manage multi-factor authentication systems
- Provide technical guidance on password security best practices

IT Staff

- Implement and maintain password management systems and tools
- Assist users with password resets and account lockouts
- Configure systems to enforce password policies
- Monitor and report on password policy compliance

Management

- Support and enforce password policies within their departments
- Ensure team members complete required password security training
- Report any password-related concerns or incidents to IT Security
- Lead by example in adhering to password best practices

Third-Party Vendors

- Comply with the organization's password requirements for accessing systems
- Implement secure password practices in any provided services or products
- Report any password-related security incidents promptly
- Participate in password security audits as required

User

- Create and use strong, unique passwords for all accounts
- Change passwords according to the organization's policy
- Never share passwords or write them down in unsecured locations
- Use multi-factor authentication when available
- Report any suspicious account activity or potential password compromises

Procedure

Passwords are an important aspect of information security. A poorly chosen password may result in unauthorized access and/or exploitation of SnowBe Online resources. All users, including contractors and vendors with access SnowBe Online systems and networks are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Password Creation

- All user-level and system-level passwords must conform to the *Password Construction Guidelines* (See below.)
- Users must not use the same password for SnowBe Online accounts as for other non- SnowBe Online access (for example: personal Internet Service Provider (ISP) account, option trading, benefits and so on.)
- Where possible, users must not use the same password for various SnowBe Online access needs.
- User accounts that have elevated privileges must have a unique password from all other accounts held by that user.

Password Change

- All passwords for user accounts with elevated privileges (for example: root, enable, NT admin, application administration accounts and so on) must be changed at least every six months.
- All user-level passwords (for example: email, web, desktop computer and so on) must be changed at least once a year. The recommended change interval is every six months.
- Password cracking or guessing may be performed on a periodic or random basis by the Security Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the *Password Construction Guidelines*.

Password Protection

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential SnowBe Online information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be left on answering machines, but rather should be shared with the intended audience in person only.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example: “my family name”.)

- Do not share SnowBe Online passwords with anyone (superior, peer or subordinate) under any circumstance.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile device (phone, table) without encryption. Refer to the SnowBe Online encryption procedure for help on encrypting password files.
- Do not use the "Remember Password" feature of applications (for example: web browsers.)
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords immediately.

Application Development

Application developers must ensure that their programs contain the following security precautions:

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in cleartext or in any easily reversible form.
- Applications must not transmit passwords in cleartext over the network.
- Applications must provide for some sort of role management such that one user can take over the functions of another without having to know the other's password. This functionality should be limited to Admin users of the system and should be approved by the system owner and documented.

Use of Passwords and Passphrases

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks." A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase: "U Mu5t B the Ch@nge U W!5h 2 C !n the W0rld" All of the rules above that apply to passwords also apply to passphrases.

Password Construction Guidelines

SnowBe Online requires a strong password that meets the following criteria:

- It must be a minimum of ten (10) characters
- It must contain three (3) of the following types of characters:
    - Uppercase letter
    - Lowercase letter
    - Numeral
    - Non-alphanumeric characters (% ! & # $ etc)
- It cannot contain a user's logon name
- It cannot contain any portion of the user's full name

Employee Creating a Password

1. Go to SnowBe Online Intranet
    a. Open your browser of choice (like Safari, Chrome, or Edge)
    b. Across the top in the address bar type in intranet.snowbeonline.com
    c. Then press enter on your keyboard.

2. Once The Website Opens
    a. If you are new: Look for a button that says, ‘Create Account’ in upper right of page and click it.
    b. If you already have an account: Look for ‘My Account’ in the upper right, then select ‘Change password’ in the drop-down menu.
3. Make Your Password
    a. Follow the password construction guidelines above to create your password.
4. Double-Check Your Password
    a. Type your new password you created again where it says ‘Confirm Password’
5. Save Your New Password
    a. Look for a button that says ‘Save; or ‘Submit’ and click it
6. You will get an email confirmation stating that your password has been created. The email address will be your company email.

IT Creates Employee Password

1. Access The User Management System
    a. After you login to your computer, open the company’s user management portal on your desktop (You will see a red circle with the letters SB in white in the middle)
    b. Log in with your IT credentials you were provided by management.
2. Locate Or Create the Employee Account
    a. For new employees: click on ‘Create new User’
    b. For existing employees: search for the employee’s name.
        i. On the top left next to search, change drop down on left of text box to ‘User’ to search for user.
        ii. Select the employee that you are looking for to change their password.
    c. When prompted to enter either a new password or change exiting user password you will need to follow the password construction guidelines above.
3. Set Password Expiration
    a. Configure password to expire after 24 hours.
        i. Unless you are creating on a Friday. Then it should be set to 72 hours to excuse the weekend allowing the employee to change it Monday when they arrive.
4. Document And Communicate
    a. Securely record the temporary password
    b. Send an email communication to the employee company email since it is encrypted, and personal emails may not be.
    c. Attach the SnowBe Online password policy and creation guidelines to the email.
5. Enable Forced Password Change
    a. Set the account to require password change when employee next login.
6. After the expiration period passes check to verify the employee logged on and changed their password. If they have not, please follow up with their immediate manager.

Resetting a Password

1. Initiate Password Reset
    a. Click on the “Forgot Password” link on the login page.
2. Enter Your Email
    a. Provide your company email address and follow the on screen instructions sent to you for resetting your password.
3. Create a New Password
    a. Set a new password that complies with the complexity rules mentioned above, then confirm your change.
4. Complete Multi-Factor Authentication (MFA)
    a. If MFA is enabled, follow the additional authentication steps to finalize your reset.

Password Expiration

1. Notification of Expiration
    a. You will receive a system notification one week before when your password is nearing expiration (90 days).
2. Reset Before Expiration
    a. Follow the same steps as above to reset your password before it expires.
3. Avoid Reusing Old Passwords
    a. Ensure that your new password is not identical to any of the last 10 passwords used.

Deleting a Password

1. Initiate Deletion Process
    a. When an employee leaves the company or no longer requires access, the supervisor or point of contact (POC) must complete the Password Deletion Form and submit it to the IT Department.
2. Account Deletion by IT
    a. The IT Department will proceed to delete or disable the account and remove the user’s password from the system.
3. Verification of Deletion
    a. A second member of the IT team will verify the deletion process for accuracy and security.

Best Practices for Password Protection

1. Keep Your Password Confidential
    a. Never share your password with anyone or write it down in an unsecured manner.
2. Avoid Browser Features
    a. Refrain from using the "Remember Password" feature in web browsers or applications for added security.
3. Report Suspicious Activity
    a. If you suspect that your password has been compromised, report it to the IT Department immediately and follow the reset procedure outlined above.

Exceptions/Exemptions

Exceptions to this Security Plan are only permissible in rare situations where strict adherence would significantly disrupt business operations.

- Any request for an exception must be made in writing to the IT Security Manager.
- The IT Security Manager will evaluate it in collaboration with pertinent stakeholders.
- If granted, the exception will be in place until the policy changes or the person's employment status changes.
- The IT Security Manager and the Risk Management team will perform a detailed risk assessment and put suitable compensation controls in place to reduce potential risks during the exception period.
- The approval of exceptions will depend on these mitigating measures.

Enforcement

Violations of this IT Security Plan will result in disciplinary actions, which may include, but are not limited to, verbal or written warnings, suspension, termination of employment, or legal action, depending on the severity of the violation.

- 1st violation, verbal coaching.
- 2nd violation, written coaching.
- 3rd violation, associate retraining.
- 4th violation, suspension.
- 5th violation, termination.

Regular audits and monitoring will be conducted to ensure compliance, and employees are encouraged to report any suspected security incidents or policy breaches to the IT Security team immediately. IT audits will be conducted monthly at discretion of the IT manager. The senior IT Manager will summarize the audit findings monthly and present it to the CISO.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	12-Nov-24	Daphnie Bruno		Created rough draft of procedure
1.2	13-Nov-24	Daphnie Bruno		Created step by step guide for internal and external users
1.3	14-Nov-24	Daphnie Bruno		Fixed Table of content and procedure
1.4	20-Nov-24	Daphnie Bruno		Finalized Document

Citations

- State of Oregon Enterprise Information Services Information Security Plan https://www.oregon.gov/eis/cyber-security-services/Documents/eis-css-statewide- information- security-program-plan.pdf
- Information Security Plan from Washington and Lee University https://my.wlu.edu/its/about-its/information-security-plan
- Grammarly, Inc. (n.d.). *Grammarly: Free writing assistant*. Retrieved from https://www.grammarly.com Used to correct grammar errors and spelling errors.
- https://rockvalleycollege.edu/_resources/files/procedures/2-30-060-Procedure-Passwords.pdf
- Cloudinary