SNOWBE ONLINE 11.15
PASSWORD PROCEDURE

Alex Fhermaye

11.15 Password Procedure – 1.0

DATE: June 30, 2024

Table of Contents

Purpose

The security of our systems and data at SnowBe is paramount. To protect our resources from unauthorized access and potential breaches, it is crucial that we adhere to strict password procedures. This document outlines the steps and guidelines for creating, using, and managing passwords within our Active Directory (AD) environment. By following these procedures, we ensure that our network remains secure and our data protected.

Scope

This password procedure applies to all employees, contractors, and third-party users who have access to SnowBe's systems and network through Active Directory. It aims to define the requirements for creating strong passwords, establish guidelines for regular password changes, provide instructions for securely recovering forgotten passwords, and ensure compliance with industry best practices and regulatory requirements. All users must adhere to these procedures to maintain the security and integrity of SnowBe's information systems. Non-compliance may result in disciplinary action and potential legal consequences. Regular audits will be conducted to ensure adherence to these procedures.

Definitions

Active Directory (AD):
A directory service developed by Microsoft for Windows domain networks. It is used for managing permissions and access to networked resources.

Authentication:
The process of verifying the identity of a user by requiring a valid username and password.

Multi-Factor Authentication (MFA):
A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity.

Password Change:
The process of updating an existing password to a new one, typically done periodically to maintain security.

Password Criteria:
The specific requirements that a password must meet, such as length, complexity, and the inclusion of various character types.

Password Manager:
A software application used to store and manage a person's passwords and strong credentials.

Password Recovery:
The process of retrieving or resetting a forgotten password using identity verification methods.

Security Questions:
Predefined questions used as an additional layer of security to verify a user's identity during password recovery.

Unauthorized Access:
Access to systems or data by individuals who do not have permission to do so.

Verification Code:
A code sent to a user via email or SMS to confirm their identity during password recovery.

Roles & Responsibilities

Chief Information Officer (CIO)

- Develop and implement the overall IT security strategy in alignment with business objectives.
- Oversee the IT department to ensure effective execution of security policies and controls.
- Ensure compliance with industry standards and regulatory requirements, including NIST 800-53 and PCI DSS.

Compliance Officer

- Ensure the company adheres to all relevant legal, regulatory, and industry standards.
- Conduct regular audits and assessments to identify compliance gaps.
- Work with other departments to implement corrective actions and maintain compliance.

IT Consultant

- Provide expert advice and guidance on IT security best practices and frameworks.
- Conduct risk assessments and develop action plans to address identified vulnerabilities.
- Assist in the implementation of security controls, policies, and procedures.

IT Security Manager

- Oversee the day-to-day operations of IT security within the company.
- Manage the IT security team and ensure the implementation of security controls and measures.
- Monitor security incidents and respond to breaches or threats.

Sales Team

- Adhere to IT security policies and procedures, particularly when accessing company systems remotely.
- Report any suspicious activities or potential security incidents to the IT security team.
- Ensure the secure handling of customer data and payment information during transactions.

System Administrator

- Manage and maintain servers, ensuring they are secure and up-to-date.
- Implement and enforce access controls to limit data access based on roles and responsibilities.
- Regularly update and patch operating systems and software to mitigate vulnerabilities.

Web Developer

- Ensure the company's website and applications are secure and up-to-date.
- Implement security measures for online transactions and data storage.
- Regularly update and patch the WordPress shopping cart and other web components.

Procedure

1. Creating a New Password

1. Log in to Active Directory:

- Open your web browser and navigate to the SnowBe Active Directory login page.
- Enter your current username and password to access your account.

2. Access Password Change Section:

- After logging in, navigate to the 'Settings' or 'Account Management' section.
- Select the 'Change Password' option.

3. Enter Current Password:

- In the designated field, enter your current password to authenticate the change.

4. Create a New Password:

- Enter a new password that meets the following criteria:
    - Minimum of 12 characters.
    - Includes at least one uppercase letter.
    - Includes at least one lowercase letter.
    - Includes at least one number.
    - Includes at least one special character (e.g., !, @, #, $).

5. Confirm New Password:

- Re-enter the new password in the confirmation field to ensure accuracy.

6. Save Changes:

- Click the 'Save' or 'Submit' button to finalize the password change.
- You will receive a confirmation message indicating that your password has been successfully updated.

2. Changing an Existing Password

1. Log in to Active Directory:

- Open your web browser and navigate to the SnowBe Active Directory login page.
- Enter your current username and password to access your account.

2. Access Password Change Section:

- Navigate to the 'Settings' or 'Account Management' section.
- Select the 'Change Password' option.

3. Enter Current Password:

- In the designated field, enter your current password to authenticate the change.

4. Create a New Password:

- Follow the same criteria for password creation as outlined above:
    - Minimum of 12 characters.
    - Includes at least one uppercase letter.
    - Includes at least one lowercase letter.
    - Includes at least one number.
    - Includes at least one special character.

5. Confirm New Password:

- Re-enter the new password in the confirmation field to ensure accuracy.

6. Save Changes:

- Click the 'Save' or 'Submit' button to finalize the password change.
- You will receive a confirmation message indicating that your password has been successfully updated.

3. Recovering a Forgotten Password

1. Navigate to the Password Recovery Page:

- Open your web browser and go to the SnowBe Active Directory login page.
- Click on the 'Forgot Password' link.

2. Verify Your Identity:

- Enter your username and follow the on-screen instructions to verify your identity.
- This may include answering security questions or receiving a verification code via email or SMS.

3. Create a New Password:

- Once your identity is verified, you will be prompted to create a new password.
- Follow the same criteria for password creation as outlined above.

4. Confirm New Password:

- Re-enter the new password in the confirmation field to ensure accuracy.

5. Save Changes:

- Click the 'Save' or 'Submit' button to finalize the password recovery.
- You will receive a confirmation message indicating that your password has been successfully reset.

4. Password Management Best Practices

1. Regular Password Changes:

- Change your password every 90 days to maintain security.

2. Avoid Password Reuse:

- Do not reuse any of your last five passwords.

3. Secure Storage:

- Do not write down your passwords or store them in easily accessible locations.
- Use a reputable password manager if necessary.

Exceptions/Exemptions

At SnowBe Online, we recognize that there may be exceptional circumstances requiring deviations from our established IT security policies. However, such exceptions/exemptions are not guaranteed approval and must be carefully evaluated to ensure they do not compromise our security posture. The following outlines the process for requesting and managing exceptions/exemptions:

How to Request an Exception/Exemption

1. All requests for exceptions or exemptions must be submitted in writing via the official IT Security Exception Request Form, available on the company net.

2. A detailed explanation of why the exception or exemption is being requested, including the specific policy or control from which the deviation is sought. The proposed duration for which the exception or exemption is needed.

Approval Process

1. The IT Security Manager will review the request to ensure it includes all required information and assess the potential risks and impacts.

2. The Chief Information Officer (CIO) has the final authority to approve or deny exceptions and exemptions. In cases involving significant risk, the CIO may consult with the Chief Executive Officer (CEO) or the IT Security Advisory Committee.

3. The applicant will be notified in writing of the decision, including any conditions or additional controls required as part of the approval.

Duration and Review

1. Approved exceptions or exemptions will typically be granted for a specified duration, not exceeding one year unless otherwise stated.

2. All active exceptions or exemptions will be reviewed periodically by the IT Security Manager to ensure that they remain necessary and that any associated risks are being adequately managed.

Enforcement

Compliance with the IT security policy and any granted exceptions or exemptions will be monitored continuously. Any deviations from approved exceptions or exemptions must be reported immediately to the IT Security Manager.

Failure to follow the IT security policy, including the proper procedure for requesting and adhering to exceptions or exemptions, may result in disciplinary actions. Penalties may include, but are not limited to, revocation of access privileges, formal reprimand, or other disciplinary actions up to and including termination of employment.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	June 30, 2024	Alex Fhermaye	Samuel Herrera	Policy created

Citations

Finalsite. (n.d.-e). https://resources.finalsite.net/images/v1706123536/sdcoenet/l2snudgl4hbtoy460lbz/SDCOEPasswordProcedures.pdf

Sandiegocounty. (n.d.-h). https://www.sandiegocounty.gov/content/dam/sdc/hhsa/programs/sd/compliance/info_security_docs/N-09_procedure_disabling-accounts-quickly_2017.10.pdf