SNOWBE ONLINE 11.14 PASSWORD STANDARD

Alex Fhermaye

11.14 Password Standard - 1.0

DATE: June 30, 2024

11.14 Password Standard – V 1.0
Status: ☒ Working Draft □ Approved □ Adopted
Document owner: Alex Fhermaye
DATE Jun 30, 2024

Table of Contents

Purpose

The purpose of this policy is to establish a comprehensive standard for the creation, management, and security of passwords within SnowBe. Effective password management is crucial to safeguarding SnowBe's sensitive information, maintaining the integrity of our systems, and protecting our organization from unauthorized access and potential security breaches. By implementing this policy, SnowBe aims to ensure that all personnel adhere to best practices in password security, thereby reducing the risk of cyber threats and enhancing overall organizational security.

Scope

This policy applies to all employees, contractors, vendors, and any other personnel who have access to SnowBe's systems, networks, and data. It encompasses all systems and applications, whether on-premises or cloud-based, that require password authentication. This includes, but is not limited to, email accounts, internal systems, cloud services, and any third-party applications used in the course of conducting business. The policy also covers the procedures for password recovery, management of administrative passwords, and the use of multi-factor authentication to ensure an additional layer of security. Adherence to this policy is mandatory for all relevant personnel to ensure a unified and secure approach to password management across the organization.

Definitions

Account Lockout:

A security measure that locks a user account after a predetermined number of unsuccessful login attempts, requiring intervention to unlock it.

Administrative Passwords:

High-level credentials that provide access to system administration functions and sensitive information, requiring higher complexity and security measures.

Contractors and Vendors:

External personnel who provide services to the company and may require access to its systems and data under strict security guidelines.

Encrypted Password Managers:

Software applications that store and manage online credentials securely by encrypting them to protect against unauthorized access.

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 for a login or other transaction.

Password:

A secret word or string of characters used for authentication to prove identity or access approval to gain access to a resource.

Security Questions:

Predefined questions used as a secondary method of authentication during the password recovery process to verify the user's identity.

Sensitive Data:

Information that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization.

Systems and Applications:

The various hardware and software components that comprise the company's technology infrastructure, requiring authentication for access.

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.

Standard

3.1 Password Creation

- Passwords must be at least 12 characters in length.
- Passwords must contain a mix of upper- and lower-case letters, numbers, and special characters.
- Passwords must not contain easily guessable information such as names, birthdates, or common words.

3.2 Password Change and Expiration

- Passwords must be changed every 90 days.
- Users will be prompted to change their password 14 days before it expires.
- Users must not reuse any of their last five passwords.

3.3 Account Lockout

- Accounts will be locked after five unsuccessful login attempts.
- Locked accounts can only be unlocked by contacting the IT helpdesk.

3.4 Multi-Factor Authentication (MFA)

- MFA is required for access to all critical systems and sensitive data.
- MFA methods may include SMS verification, email verification, or authentication apps.

3.5 Password Storage

- Passwords must never be written down or stored in plain text.
- Passwords must be stored using secure, encrypted password managers approved by the IT department.

3.6 Password Recovery

- Password recovery procedures must verify the identity of the user before allowing a password reset.
- Users must answer security questions or use MFA to recover or reset passwords.

3.7 Administrative Passwords

- Administrative passwords must adhere to higher complexity and length requirements, as determined by the IT department.
- Administrative passwords must be changed every 60 days.

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

Password policy - jonesboro.org. (n.d.-e). https://www.jonesboro.org/DocumentCenter/View/4253/Password-Policy-PDF

University, T. S., & Cit. (n.d.). *Undergraduate*. Password Policy. https://www.tnstate.edu/cit/password_policy.aspx

11.15 - password policy. Information Technologies & Services. (n.d.). https://its.weill.cornell.edu/policies/1115-password-policy