SNOWBE ONLINE

Password Standard

Your name: Jalif Vazquez

Password Standard

Version #1.2

DATE:12/21/24

Table of Contents

Purpose

The SnowBe's Password Standard is designed to protect the organization's information systems by ensuring that non-organizational users adhere to best practices in password management. This includes guidelines for password creation, usage, and maintenance to safeguard sensitive data against unauthorized access.

The purpose of this Password Standard is to establish guidelines for the creation, use, and management of passwords to ensure the confidentiality, integrity, and availability of SnowBe's information. This Standard provides the rules for generating secure passwords and the importance of adhering to these practices to protect sensitive data.

The Password Standard exists to define the requirements for creating, managing, and using passwords within the SnowBe environment. It aims to enhance the security of user accounts and protect sensitive information from unauthorized access. A strong password policy minimizes risks associated with data breaches and unauthorized user access.

Scope

The following contains rules governing password creation and management. Implementing the SnowBe Password Standard is critical for maintaining the integrity, confidentiality, and availability of the organization's information. By following these guidelines, both the organization and its users can significantly reduce the risk of data breaches and enhance overall security posture. This Standard applies to all non-organizational users who access SnowBe systems. This includes but is not limited to external partners, vendors, contractors, and any user granted access to SnowBe resources

Definitions

Assumed Breach: The model operates under the assumption that there may already be a breach within the network, prompting heightened security measures.

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

Continuous Monitoring: Ongoing surveillance of user activity and access patterns helps detect and respond to anomalies in real-time.

Encryption: The method of encoding information so that only authorized parties can access it.

Identity Verification: Every access request must be authenticated and authorized using multi-factor authentication (MFA) wherever possible.

Least Privilege Access: Users and devices are granted the minimum level of access necessary to perform their tasks, reducing the risk of unauthorized access.

Micro-Segmentation: Networks are divided into smaller, isolated segments, limiting lateral movement within the network.

Password: A secret word or phrase used for user authentication to gain access to a system.

Security Team: Responsible for reviewing and updating the Standard as necessary, along with monitoring compliance.

System Administrators: Responsible for enforcing password policies and managing user accounts.

Users: Responsible for creating, managing, and protecting their passwords by this Standard.

Roles & Responsibilities

Audit Team: The Audit Team ensures the effectiveness of security controls through regular evaluations. They review logs, processes, and reports, identifying areas for improvement and recommending changes to ensure compliance with SnowBe Online's policies and regulatory standards.

Chief Information Security Officer (CISO) OR Security Lead: The CISO or Security lead is responsible for establishing and overseeing SnowBe Online's security strategy, ensuring it aligns with business objectives and regulatory requirements. This role involves conducting risk assessments, developing mitigation strategies, approving security policies, and supervising their implementation.

Compliance Officer: The Compliance Officer ensures that SnowBe Online follows all relevant regulatory standards, including PCI DSS and NIST 800-53. This role involves managing audit preparations, documenting compliance activities, and working with other departments to implement required controls, ensuring the company remains compliant with all applicable laws and standards.

End Users (Employees): All employees are responsible for complying with SnowBe Online's security policies and using company systems in a secure and responsible manner. This includes participating in regular security awareness training, safeguarding credentials, and reporting phishing attempts or suspicious activities. Remote employees are required to use secure methods, such as VPNs, to access internal company systems.

Executive Leadership: Executive leadership is responsible for providing all necessary resources. They promote adherence to security policies across the organization and approve any significant changes to security practices or business processes.

Incident Response Team: The Incident Response Team is tasked with handling security incidents and minimizing potential damage to the company. They investigate root causes, document findings, and update the incident response plan as needed. The team also conducts regular exercises to ensure readiness for future incidents.

IT Manager/Infrastructure Team: The IT Manager is responsible for maintaining and securing the company's IT infrastructure, which includes servers, desktops, laptops, and network devices. This involves ensuring all devices are updated with the latest hardware and software, securing physical assets like on-premises servers, and overseeing the implementation of disaster recovery processes.

Network Administrators: The Network Administrators secure and manage all network devices, including firewalls, routers, and switches. They ensure the network infrastructure is updated, segmented appropriately, and monitored for potential threats. They also establish secure remote access solutions, such as VPNs, and maintain activity logs for auditing and forensic purposes.

Security Analyst: The Security Analyst plays a vital role in identifying and mitigating security risks. This involves conducting vulnerability scans, penetration tests, and regular risk assessments. The Security Analyst monitors the organization's systems for potential threats, investigates incidents, and provides actionable recommendations to improve SnowBe Online's security posture.

System Administrators: System Administrators are responsible for the secure operation of SnowBe Online's on-premises and cloudbased servers (AWS). Their duties include implementing access controls based on the principle of least privilege, deploying and managing antivirus solutions, and maintaining critical systems such as the WordPress shopping cart to ensure reliable and secure operations.

Retail Staff: Retail staff are responsible for securely handling customer credit card transactions at physical storefronts. This includes following company policies for payment terminal use and ensuring customer data is processed securely. They are also expected to report any suspicious activities or system anomalies to the appropriate teams.

Technical Consultant (external role): The Technical Consultant provides expertise in identifying and mitigating risks, helping SnowBe Online implement the NIST 800-53 framework, as well as other industry best practices. This includes assisting with system hardening, process improvements, and deploying technical controls to address identified vulnerabilities.

Third Party Vendors: Third-party vendors are responsible for adhering to SnowBe Online's security policies and contractual obligations. They must ensure the security of the services and systems they provide, cooperate during audits, and supply any required documentation to verify compliance with regulatory and contractual requirements.

Standard

- All be performed to identify potential security threats and inform necessary policy adjustments.

- All SnowBe’s employees and partners are responsible for safeguarding their system access login credentials and must comply with the password standards outlined in this policy.

- Passwords must not be shared with anyone and must be created and maintained by these guidelines.
  (Following the password procedures stated.)

- Passwords must be at least 12 characters long and include a mix of upper- and lower-case letters, numbers, and special characters.

- Passwords must not contain easily guessable information such as names or birthdays.

- Passwords should be changed every 90 days.

- Users should not reuse passwords across different platforms or applications.

Exceptions/Exemptions

- Requests must be formally submitted to the IT Director, specifying the security controls affected.

- Following submission, the request will be reviewed by senior management and the legal team.
  If approved, the exception will be temporary, lasting up to 45 days.

- During this exception period, the IT team will implement necessary risk mitigation measures and monitor for any escalating risks.

- After 45 days, the exception will either expire, necessitating a return to full compliance, or the request will be reassessed for a potential extension.

- If no extension is granted, the IT team will ensure all temporary adjustments are removed and that the system fully adheres to the original security controls

- Emergency circumstances: In very urgent situations such as a system recovery, there should be certain security protocols that might need to be temporarily bypassed. If this situation occurs, it must be clearly documented and justified as to why it was performed.

- Role-based exceptions: In specific rules such as the system administrators, they might need exceptions to standard rules. An example of this could be broader access to the systems. These roles could come with additional oversight and security measures and must be used with proper documentation.

- Third-Party services: If a third-party would happen to be needed a security plan must allow for that specific service. This is only if the provided met predefined security standards as well as passed audits.

Enforcement

Enforcing this security policy is crucial for maintaining the integrity and confidentiality of SnowBe Online's information systems. The System Administrator at SnowBe Online has the authority to restrict or suspend access for individuals who do not comply with the established security policies and procedures. In situations presenting immediate threats, the IT Director can revoke access rights entirely for any parties involved to safeguard the integrity of SnowBe Online’s systems.

Violations of security policies may lead to the suspension or termination of system access. Additionally, when appropriate, civil or criminal penalties may be pursued. Disciplinary actions will be determined based on the severity of the offense and the individual's compliance history. Policy Enforcement Procedures To uphold the integrity and confidentiality of SnowBe Online's information systems, strict enforcement of security policies is vital.

The following outlines the actions that may be taken in response to policy violations:

1. Verbal Reprimand - For minor, first-time offenses that pose minimal risk or damage, a verbal warning will be issued. This serves as a reminder about the importance of following security protocols.

2. Written Warning/Documentation - A formal written warning will be provided for more serious or repeated offenses. This documentation will specify the nature of the infraction and outline necessary corrective actions. It will be added to the employee's performance record.

3. Mandatory Training - Employees who repeatedly violate security policies or demonstrate a lack of understanding may be required to undergo additional cybersecurity training. Completion of this training will be essential for maintaining system access and employment.

4. Suspension of Access or Employment - In cases of severe infractions or ongoing non-compliance, employees may face a temporary suspension of their system access or employment. The System Administrator or IT Director will make this decision and will remain in effect until a comprehensive review and investigation are completed.

5. Termination of Employment - Serious violations resulting in data breaches, financial loss, or substantial harm to SnowBe Online may lead to employment termination. This process will follow a formal investigation conducted by the security and IT teams.

6. Legal Action - In cases where violations lead to criminal activities or breaches of regulatory compliance, SnowBe Online retains the right to pursue civil or criminal penalties and employment-related consequences.

SnowBe Online aims to maintain a safe and secure working environment by adhering to these enforcement procedures.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.2	12/11/24	Jalif Vazquez		Physical Access Control.
1.3	12/21	Jalif Vazquez		Password Standard

Citations

NIST Special Publication 800-63B: Digital Identity Guidelines
https://pages.nist.gov/800-63-3/sp800-63b.html

1.15 - Password Policy
https://its.weill.cornell.edu/policies/1115-password-policy