SNOWBE ONLINE

Policy# SP-02

Password Policy

Daphnie Bruno

Policy #SP-02 - Version # 1.1

November 01, 2024

Table of Contents

PURPOSE 2

SCOPE 2

DEFINITIONS 2

ROLES & RESPONSIBILITIES 5

POLICY 6

EXCEPTIONS/EXEMPTIONS 7

ENFORCEMENT 8

VERSION HISTORY TABLE 8

CITATIONS 9

Purpose

This policy is to educate SnowBe Online staff on the characteristics of a strong password as well as to provide recommendations on how to securely maintain and manage passwords. The purpose of this policy is to establish a strong password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software.

Scope

This policy applies to all employees, guests, contractors, partners, vendors that have a username and password to at least one SnowBe Online system or application, independent of whether you are an end user or a system administrator for that system or application.

Definitions

Adhere/Adhering

To follow or comply with a rule, guideline, or policy strictly.

Characteristics

Typical features or qualities of something, in this context, attributes of strong passwords.

Circumvent

To bypass or find a way around a rule, policy, or security measure.

Compensation

In security context, measures taken to offset or offset a weakness or vulnerability.

Compliance

The state of conforming to rules, regulations, or policies.

Compromised

When referring to accounts or passwords, it means they have been accessed or obtained by unauthorized parties.

Consultation

The process of seeking advice or discussing matters with relevant parties before planning.

Discretion

The freedom to make decisions within certain limits; in IT, often refers to the authority to make judgment calls.

Disciplinary

Relating to actions taken to correct or punish misconduct or policy violations.

Encrypted

Data that has been converted into a code to prevent unauthorized access.

Implemented

Put into effect or action, such as deploying a new policy or system.

Independent

Not influenced or controlled by others, independent in function or decision-making.

Integrity

In IT security, the declaration that data has not been tampered with or altered without authorization.

Justification

The action of showing something to be right or reasonable, providing valid reasons for a decision or action.

Mitigating

Reducing the severity or seriousness of something, often referring to security risks or threats.

Permissible

Allowed or acceptable within the rules or policies.

Pertinent

Relevant or applicable to a particular matter.

Questionnaires

A set of written questions used to gather information, often used in security assessments.

Reasonably

To a fair or moderate extent; within acceptable limits.

Recommendations

Suggestions or proposals put forward with supporting reasons.

Severity

The seriousness or intensity of something, often used to classify security incidents or policy violations.

Specialized

Designed for or requiring specific skills, knowledge, or training.

Violation

The action of breaking or failing to comply with a rule, agreement, or policy.

Roles & Responsibilities

Contractors/Vendors

- Required to inform their point-of-contact at SnowBe Online when their passwords are no longer needed.
- Must comply with the same password creation and protection standards as the SnowBe Online employees.

Employees

- SnowBe Online Employees are responsible for adhering to password creation and protection standards.
- Employees must notify their immediate supervisor if a password is no longer needed or if their account is suspected to be compromised.
- All SnowBe Online Employees must change their passwords every 90 days and avoid password reuse from the last 10 passwords.

Information Security Department

- The Information Security Department must perform monthly and random password-guessing tests to identify weak passwords.
- Information Security Department will ensure the integrity and security of password management policies and practices.

IT Security Manager

- The IT Security Manager at SnowBe Online is responsible for the deletion of user passwords and suspension of user accounts once notified by the relevant supervisor or contractor.
- SnowBe Online will conducts bi-monthly regular password cracking or guessing audits and ensures compromised passwords are changed.
- The IT Security Manager will review and approve any requests for password-related exceptions or exemptions in consultation with stakeholders.

Policy

Passwords for SnowBe Online network access must be implemented according to the following policy:

- Passwords must be changed every 90 days.
- Passwords must adhere to a minimum length of 10 characters.
- Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits (!@#$%^&*_+=?/~’;’,<>|\).
- Passwords must not be easily tied back to the account owner such as:
  - Username, social security number, nickname, relative’s names, birth date, etc.
- Passwords must not be dictionary words or acronyms.
- Passwords cannot be reused for 1 year.

All system-level passwords at SnowBe Online must adhere to the following guidelines:

- Passwords must be changed at least every 6 months.
- All administrator accounts must have 12-character passwords which must contain three of the four items: upper case, lower case, numbers, and special characters.
- Non-expiring passwords must be documented listing the requirements for those accounts. These accounts need to adhere to the same standards as administrator accounts.
- Administrators must not circumvent the Password Policy for the sake of ease of use.

The Password Protection guidelines have also been added to the Policy:

- The same password must not be used for multiple accounts.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential SnowBe Online information.
- Stored passwords must be encrypted.
- Passwords must not be inserted in e-mail messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords must not be revealed on questionnaires or security forms.
- Users must not hint at the format of a password (for example, “my family name”).
- SnowBe Online passwords must not be shared with anyone, including co-workers, managers, or family members, while on vacation.
- Passwords must not be written down and stored anywhere in any office. Passwords must not be stored in a file on a computer system or mobile device (phone, tablet) without encryption.

- If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:
    - Take control of the passwords and protect them.
    - Report the discovery to IT.
- Users cannot circumvent password entry with an auto logon, application remembering, embedded scripts, or hard-coded passwords in client software. Exceptions may be made for specific applications (like automated backup processes) with the approval of IT. For an exception to be approved, there must be a procedure to change the passwords.
- PCs must not be left unattended without enabling a password-protected screensaver or logging off the device.
- If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:
    - Take control of the passwords and protect them
    - Report the discovery to IT
- Security tokens (i.e. smartcards, RSA hardware tokens, etc.) must be returned upon demand or upon termination of the relationship with SnowBe Online.

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	30-Oct-24	Daphnie Bruno		First Draft of Password Policy
1.1	01-Nov-24	Daphnie Bruno		Finalized after feedback

Citations

UC Berkley

Information Security Office

IBM

PurpleSec

Murray State University

Grammarly, Inc. (n.d.). *Grammarly: Free writing assistant*. Retrieved from https://www.grammarly.com
Used to correct grammar errors and spelling errors.