SNOWBE ONLINE

Standard# PS-01

Password Standard

Daphnie Bruno

Standard #PS-01 | Version # 1.1

November 19, 2024

Table of Contents

Purpose

This standard identifies the minimum password requirements needed to protect SnowBe Online data and systems. Passwords are used on SnowBe Online devices and systems to facilitate authentication, i.e., helping ensure that the person is who they say they are. The security of SnowBe Online data is highly dependent upon the secrecy and characteristics of the password. Compromised passwords can result in loss of data, denial of service for other users, or attacks directed at other Internet users from a compromised machine. Compromised passwords can also result in the inappropriate disclosure of private data such as research participant data, and private employee data.

Scope

These standards apply to all electronic devices and systems connected to SnowBe Online network including computers, network switches and routers, personal digital assistant devices, laptop computers, password authenticated software, etc.

Definitions

The definitions provided below are integral to the terms used in the Password Standard documentation. A comprehensive understanding of these terms is crucial for the effective implementation and accurate interpretation of this standard.

Adherence:
The act of following or sticking to a rule, policy, or principle

Authenticated:
Verified or confirmed as genuine or valid

Authentication:
The process of verifying the identity of a user, system, or entity before granting access to resources.

Availability:
The state of being accessible, usable, or ready for use

Compromised:
Weakened or damaged, especially in terms of security or integrity

Confidentiality:
The state of keeping information private or secret

Consecutive:
Following one after another in order without interruption

Disclosure:
The act of revealing or making information known

Electronic:
Related to or operated by electricity or electronic technology

Facilitate:
To make easier or help bring about

Inappropriate:
Not suitable or proper in a particular situation

Inactivity:
The state of not being active or in use

Integrity:
The state of being whole, undivided, or uncompromised

Non-compliance:
Failure to act in accordance with a rule, regulation, or requirement

Permitted:
Allowed or authorized

Predetermined:
Established or decided in advance

Preserve:
To maintain or keep something in its original state

Procedures:
A series of actions or steps taken to accomplish a specific task

Requirements:
Things that are needed or essential

Reserves:
Keeps or holds back for future use

Requirements:
Things that are needed or essential

Roles & Responsibilities

This section outlines the specific roles and responsibilities associated with implementing, maintaining, and enforcing the Password Standard across our organization. Clear explanation of duties ensures effective password management, enhances security, and promotes accountability at all levels.

Chief Information Security Officer (CISO)

- Oversee the development and implementation of the password policy
- Ensure alignment with overall information security strategy
- Approve final password standards and any exceptions
- Report on password security to executive management

Compliance Officer

- Ensure password standards meet regulatory requirements
- Monitor compliance with password policy across the organization
- Conduct regular audits of password practices
- Report compliance issues to management

Customer Service

- Assist users with password-related issues
- Follow secure procedures for password resets
- Educate customers on password best practices
- Escalate potential security incidents related to passwords

Employees

- Create strong, unique passwords for all accounts
- Change passwords according to policy requirements
- Never share passwords or write them down
- Report any suspicious password-related activity

Human Resources

- Include password policy in employee onboarding and training
- Enforce password policy as part of employee agreements
- Coordinate with IT for account provisioning and deprovisioning
- Handle disciplinary actions for password policy violations

IT Security Manager

- Develop and maintain the technical aspects of the password policy
- Implement password management tools and systems
- Monitor password strength and usage across the organization
- Investigate and respond to password-related security incidents

IT Security Officer

- Provide guidance on password best practices and emerging threats
- Conduct risk assessments related to password security
- Recommend updates to password policy based on security landscape
- Oversee password-related security awareness programs

IT Staff

- Configure systems to enforce password policy requirements
- Manage password reset processes and tools
- Monitor for suspicious password activity
- Provide technical support for password-related issues

Management

- Support and enforce the password policy within their departments
- Ensure employees have necessary resources to comply with policy
- Address non-compliance issues promptly
- Incorporate password security into departmental processes

IT Security

- Implement technical controls to enforce password policy
- Conduct regular password audits and vulnerability assessments
- Monitor for password-related threats and breaches
- Provide technical expertise for password management solutions

Third-Party Vendors

- Adhere to organization's password standards when accessing systems
- Implement comparable password security measures in their own systems
- Report any password-related security incidents promptly
- Participate in password security audits as required

User

- Create and maintain strong, unique passwords for all accounts
- Follow password change and reset procedures
- Never share passwords or store them insecurely
- Report any suspicious password-related activity immediately

Standard

The following standards set the minimum requirements for passwords on any SnowBe Online Information Technology (IT) resource:

• Passwords must have a minimum length of 8 characters or the maximum length the system supports if the system has a maximum password length of less than 8 characters.

• Passwords must meet at least 3 out of the 4 requirements for quality:

  o At least 1 lower case letter
  o At least 1 upper case letter
  o At least 1 number
  o At least 1 special character (?, *, %, etc.)

- Users must choose unique passwords that are difficult to guess. Passwords must not:
    - Contain the user's first name, middle name, last name, or username
    - Be based on a single dictionary word
    - Contain more than 2 repetitive characters (e.g., Mmmmmm1, Ab7777777, etc.)
    - Be a repeat of a password used within the last year
    - Be shared with other users
- Passwords on sensitive IT systems must be changed, at a minimum, every 90 days.
- Initial passwords must be unique and provided through a secure manner and changed upon first logon.
- After multiple unsuccessful consecutive logon attempts (e.g., incorrect passwords) the user's account may become automatically locked. Users may need to contact the Help Desk for account unlocking or accounts may automatically unlock after 24 hours.
- Passwords should never be written down and left in plain sight. If a password must be written down it should be stored in a secured location.
- Passwords should never be stored electronically in plaintext. A password manager should be used to securely store passwords electronically.
- Users must log off of applications when done using them.
- Users must secure workstations when they are away from them. Devices will be subject to lockouts for inactivity after 10 minutes.
- Users must only use their SnowBe Online ID and password for SnowBe Online systems and services. Users should create a different username and password for external services such as personal e-mail, banks, online stores, personally owned computers, or other systems.
- Users must report suspected password compromises by contacting the IT Help Desk.
- Users must change their password if they suspect it has been compromised.

Remote Access Users

Remote access to information technology resources (switches, routers, computers, etc.) and to sensitive or confidential information (social security numbers, credit card numbers, bank account numbers, etc.) is only permitted through secure, authenticated and centrally managed access methods.

Related Information

Adherence to password requirements is reviewed as part of the normal SnowBe Online audit procedures. SnowBe Online reserves the right to suspend account holders' access to preserve the confidentiality, integrity and availability of the SnowBe Online network, systems or information if found in non-compliance.

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	14-Nov-24	Daphnie Bruno		Created and updated Document.
1.1	19-Nov-24	Daphnie Bruno		Finalized and cleaned up document

Citations

- https://www.mtu.edu/it/security/policies-procedures-guidelines/password-standards.pdf
- Grammarly, Inc. (n.d.). *Grammarly: Free writing assistant*. Retrieved from https://www.grammarly.com
    - Used to correct grammar errors and spelling errors
- 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
- https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-program/password-standards/