SNOWBE ONLINE Policy PS-1

Password Standard POLICY

Group 2 Members:
Emma McClung

Version 2.0

DATE: 12/18/2025

Table of Contents

Purpose

This standard identifies the minimum password requirements needed to protect SnowBe data and systems. Passwords are used on SnowBe devices and systems to facilitate authentication, i.e. helping ensure that the person is who they say they are. The security of company 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 private

Scope

This plan applies to all SnowBe employees, contractors, systems, servers, mobile devices, AWS-hosted services, retail locations, laptops using VPN, and all customer-facing platforms.

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

Definitions

Keyed hash: A keyed hash is a type of message authentication code (MAC) calculated using a specific algorithm involving a cryptographic hash function in combination with a secret key.

SNMP: Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an Application Layer protocol, a database schema, and a set of data objects.

SNMP Community String: A SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.

Sudo: A unix command, the sudo command stands for "superuser do". It prompts for a personal password and confirms the request to execute a command by checking a file, called sudoers, which the system administrator configures. Using the sudoers file, system administrators can give certain users or groups access to some or all commands without those users having to know the root password. It also logs all commands and arguments so there is a record of who used it for what, and when.

Roles & Responsibilities

IT Security: Implements, monitors, and reviews all access control mechanisms and privileged accounts.

System Administrators: Apply changes, manage permissions, and maintain secure configurations.

Employees: Follow assigned access privileges and report unusual access activity.

Management: Approves access requests and oversee separation of duties processes.

Policy

Users, admin, and service accounts within Active Directory, plus accounts not through active directory, must use passwords that are a minimum of 15 characters long. They cannot use personal information i.e. birthday, address, name. All passwords must be treated as confidential information, so they cannot be written down or stored in unsecured locations. They will not be shared with anyone, transmitted through unencrypted email or electronics. Passwords must not be stored on portable devices unless they are secured and protected with an encrypted password management app. Users must notify technology services if there is any suspicious activity that suggests a password has been compromised.

Procedure

Password Creation

All user, administrative, and service accounts within Active Directory and accounts not managed through Active Directory shall be configured to require passwords with a minimum length of fifteen (15) characters. Passwords must not be based on personal information such as names, birthdays, or addresses.

Password Protection and Handling

Users must treat all passwords as confidential information. Passwords shall not be written down or stored in unsecured locations, shared with any individual, or transmitted through unencrypted email or electronic communication methods.

Password Storage

Passwords must not be stored on portable electronic devices unless they are protected by a secure, encrypted password management application approved by Technology Services.

Monitoring and Reporting

Users are required to remain alert for suspicious activity that may indicate password compromise and must immediately notify Technology Services upon discovery or suspicion of unauthorized access or credential exposure.

Exceptions/Exemptions

Exceptions to, or exemptions from, any provisions of the Security Plan and/or supplemental policies, standards, or guidelines must be approved by SnowBe's Information Technology Manager or higher. Any questions about the contents of this plan and/or supplemental policies, standards, or guidelines should be referred directly to the Information Technology Manager or a member of the department who has the responsibility to interpret the security standard. Please submit the following:

- A written document with reasoning
- Length of exemption/exception (cannot be longer than 30 days).
- Signed by the requester
- Signed by the requester's manager
- Signed by the requester's department head

Enforcement

All SnowBe employees, including the CEO, CFO, CIO, CTO, as well as remote employees, temporary employees, volunteers, guests, contractors, agents, and any third parties acting on behalf of SnowBe, are required to comply with SnowBe policies, standards, and guidelines. Should you be found in violation, you may be subject to the following disciplinary actions:

- Verbal warning
- Write-up
- Meeting with IT Manager/Mandatory Training
- Termination and/or legal action

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1	12/1/25	Group 2 members	Group 2 Leader	Entered clause for Exceptions/Exemptions
2	12/18	Group 2 members	Emma McClung	Password standards PS-1

Citations

Michigan Tech Information Technology. (2016). *Password standards*. https://www.mtu.edu/it/security/policies-procedures-guidelines/password-standards.pdf (purpose & scope)

Unknown. (2021). *Password Policy* (pp. 1–2). https://www.tscalliance.org/wp-content/uploads/2017/01/Password-Policy-Signed.pdf (policy)

President's Cabinet. (2008). CAPITAL UNIVERSITY PASSWORD POLICY. In *CAPITAL UNIVERSITY*. https://www.capital.edu/media/35edxtno/passwordpolicy20409.pdf (definitions)

OpenAI. (2025). *ChatGPT* (GPT-5.2) [Large language model]. https://chat.openai.com/

(polishing language)