a

SNOWBE ONLINE #003

Password Standard

Sean Redding

Password Standard -

Version#1.0 10-25-25

Table of Contents

Purpose

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

Scope

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

Definitions

N/A

Roles & Responsibilities

The IT Director, supported by the IT Manager, is responsible for implementing and enforcing this Standard.

Standards

The following standards must be adhered to: Procedure #004 – Password Procedure for

Snowbe Online Information Technology (IT) systems.

Remote Access:

Refer to Policy #004 - Remote Access (AC-17)

Exceptions/Exemptions

Requests for an exception must be submitted in writing to consult with the IT Director or IT Manager.

The request must be detailed with information, including:

- Length of time
- Policy or standard
- Reason

Each request will be reviewed by the IT Manager or IT Director to determine whether an exemption is justified and whether it will require compensating controls.

If the non-compliance is due to a better solution, an exception is still required and will be formally evaluated and approved.

The IT Director and the Commissioner must maintain constant communication during the exception. If approved, the Commissioner's office will send the letter of approval to the requester with details. In the event of denial, a letter of explanation will be sent to the requester with the reason the IT Director denied the request and an explanation.

Exemptions:

Access Control – Access controls, including Single Sign-On (SSO), Multi-Factor Authentication (MFA), Sessions, and IAM policies, are not to be paused or discontinued.

Enforcement

- Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director.
- Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
- Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from SnowBe.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	10-25-25	IT Director	IT Director	Initial draft of Standard.

Citations

https://www.mtu.edu/it/security/policies-procedures-guidelines/information-security-program/password-standards/ - Used for Scope, Standard, and purpose

https://it.wvu.edu/policies-and-procedures/acceptable-use/password-standard - Used for Definitions and