SNOWBE ONLINE Standard#AP-2 Password Standard

**Michael Kohronas:**

**<Password Standard>**

**Version #3**

**DATE: 06/2024**

Table of Contents

[Standard 2](#_Toc170425784)

[Scope 2](#_Toc170425785)

[Definitions 2](#_Toc170425786)

[Roles & Responsibilities 3](#_Toc170425787)

[Standard 3](#_Toc170425788)

[Exceptions/Exemptions 4](#_Toc170425789)

[Enforcement 5](#_Toc170425790)

[Version History Table 5](#_Toc170425791)

[Citations 6](#_Toc170425792)

Standard

Assigning unique individual logins and requiring password protection is one of several primary safeguards employed to restrict access to the SnowBe networks, systems, applications, and data. If a password is compromised, inappropriate access might be obtained by an unauthorized individual. Individuals with SnowBe Accounts are responsible for safeguarding against unauthorized access to their account, and as such, must conform to this Procedure in order to ensure passwords are kept confidential and designed to be complex and difficult to guess. The parameters in this Procedure are designed to comply with relevant legal and regulatory standards, including but not limited to the Payment Card Industry Data Security Standard (PCI DSS).

Scope

The SnowBe Password Standard applies to all employees creating an account or modifying their passwords. This Standard also applies to service, automated, and all accounts within SnowBe’s network. This will ensure that all within SnowBe accounts are secured with strong passwords.

Definitions

**Default Password –** A factory-set password provided by SnowBe’s IT team for initial system or device setup.

**Mobile Device Management (MDM) –** A technology methodology used by SnowBe to oversee, manage, and secure the company’s mobile devices that are deployed across various locations.

**PCI DSS Compliant –** Refers to SnowBe’s adherence to the Payment Card Industry Data Security Standard, ensuring that all credit card information handled is safely processed and handled.

**Service Accounts** **–** Specialized accounts that is used by SnowBe to run and operate application software and services.

**Test Accounts –** Accounts specifically created by SnowBe for the reason of testing the functionality or security of one of their systems.

**Temporary Password –** A limited time password that is issued when initially setting up accounts or during password resets.

Roles & Responsibilities

**All Employees, contractors, or interns –** All employees, contractors, and contractors are required to follow SnowBe’s password standard and ensure that their password meets the minimum security requirements of this standard.

**CISO –** Oversees and ensures that the password standard that was created covers all requirements for a strong password.

**IT Security team –** Monitors and ensures that all passwords are up to standard and that there aren’t any duplicates by comparing hashes and reaches out to any employee, contractor, or intern if there is any discrepancies with their password.

# Standard

All individuals are responsible for safeguarding their system access login password credentials and must comply with the password standards identified in this standard. Passwords must not be shared with or made available to anyone in any manner that is not consistent with this Procedure.

**Password Requirements:**

The following parameters indicate the minimum requirements for passwords for all accounts (except for passcodes defined in *Service Accounts and Test Accounts* below):

* At least sixteen (16) characters.
* Unique and different from passwords used for other services (e.g., personal banking or email).
* Changed at the regularly scheduled time interval as defined in this Procedure or upon suspicion or confirmation of compromise.
* Not based on anything somebody else could easily guess or obtain using person-related information (e.g., names, telephone numbers, dates of birth, etc.).
* Not reasonably vulnerable to a dictionary or brute-force attack (see Recommendations for Creating Compliant Passwords below).
* Not reused for at least six (6) generations; and,
* Significantly dissimilar to any previous passwords.

**Mobile Device Password Requirements**

Mobile devices accessing or storing SnowBe data, such as smartphones and tablets, shall be registered with ITS and managed by the mobile device management (MDM) platform. The following minimum passcode Procedure is in effect for all mobile devices:

* At least six (6) numeric digits;
* No repeating or sequential digits (e.g., 111111, 123456, or 101010); and,
* The passcode may not be one of three previously used passcodes.
* Biometric authentication (e.g., facial or fingerprint recognition) on mobile devices may be used to unlock the device, but a compliant passcode must still be established.
* Pattern unlocks or other authentication methods are not permitted.
* A mobile device must be configured to wipe/erase itself after ten (10) invalid passcode attempts. This will result in the device resetting to factory defaults with all applications and data lost in the process. The device manufacturer may automatically impose time limitations after several unsuccessful passcode attempts before the wipe is triggered. ITS Support can provide assistance in resetting device passcodes.

**System Processing Passwords**

All SnowBe systems—including, but not limited to, servers, applications, and websites that are hosted by or for SnowBe—must be designed to accept passwords and transmit them with proper safeguards.

* Passwords should be prohibited from being displayed when entered, although it is suitable to have a method to toggle visibility as needed.
* Passwords must never be stored in clear, readable format. Reasonably strong, brute-force resistant hashing methods or encryption must always be used. Hashing, including salting and peppering (if possible), should be used in lieu of encryption.
* Hashed or encrypted passwords must never be accessible to unauthorized individuals.
* Passwords must never be stored as part of a login script, program, or automated process.
* Where any of the above items are not supported, a variance request should be submitted to ITS for review pursuant to ITS policy 11.20 – Variances. Appropriate authorizations and access control methods must be implemented to ensure only a limited number of authorized individuals have access to passwords.

Exceptions/Exemptions

Exceptions to this Standard will be considered on a case-by-case basis and do not guarantee approval. To request an exception, please submit a written request to the IT Director outlining the following:

How to Request Exceptions/Exemptions?

To request an Exception or Exemption from a Standard that is in place please message ITDirector@SnowBe.com with the following format:

What Exception/Exemption are you requesting?

Why are you requesting this Exception?

How long are you requesting this Exception/Exemption for?

The IT Director, in consultation with relevant stakeholders, will review the request and determine if an exception can be granted. The decision will be based on the potential impact on security, the justification provided, and the availability of alternative secure solutions. Exceptions/Exemptions are subject to change at any point in time to strengthen security posture

Enforcement

The failure to comply with policies, standards, or Standards will result in a warning or disciplinary action depending on the severity of the infraction.

Version History Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version #** | **Implementation Date** | **Document Owner** | **Approved By** | **Description** |
| v1 | 06/06/2024 | Michael Kohronas |  | Added the exception and exemption and enforcement as a group |
| V2 | 06/07/2024 | Michael Kohronas |  | Fixed issues with text size and font, added name and date to header, |
| V3 | 06/24/2024 | Michael Kohronas |  | Added Password Standard Information |
|  |  |  |  |  |

Citations

<https://its.weill.cornell.edu/policies/1115-password-Procedure>