<Standards: New Password Creation> - V 1.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted

Document owner: SnowBe Online

Last Review Date: 09/24/2022

STAN01 - New Password Creation

Standards

Table of Contents

1. Purpose

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

2. Scope

These procedures shall apply to all employees, vendors, contractors, and affiliates of SnowBe Online.

3. Definitions

Dictionary Attack
A type of attack that relies on our habit of picking words that are personally important to you, like a birthplace, child's name, or pet's name and incorporating them as a password, in part or in full.

Payment Card Industry (PCI) Users
PCI Users are users responsible for processing payments in SnowBe Online's financial systems, such as Epic, must adhere to the Payment Card Industry's (PCI) Data Security Standard for password expiration.

Privileged Users
Privileged users consist of users with elevated access to administer information systems and applications (other than to a local device), most often in the Information Technologies & Services Department. Such users have administrator access via a shared account or to multiple systems at SnowBe Online and these accounts are at a higher risk for compromise.

Service Accounts
Service accounts are accounts used by a system, task, process, or integration for a specific purpose.

Standard Users
Standard users consist of SnowBe Online staff (including temps and consultants), and customers that are not (1) system administrators or (2) processing credit card payments.

Test Accounts
Test accounts are accounts used on a temporary basis to imitate a role, person, or training session.

4. Roles and Responsibilities

4.1. Information Owners

Information owners are responsible for:

- The implementation of these standards and all other relevant policies within the SnowBe Online organization or service they manage.
- The ownership, management, control and security of SnowBe Online information

systems used by their directorate or service to process information on behalf of SnowBe Online.
- Maintaining a list of SnowBe Online information systems and applications which are managed and controlled by their directorate or service.
- Making sure adequate procedures are implemented within their directorates or services, so as to ensure all SnowBe Online employees, third parties and others that report to them are made aware of and are instructed to comply with this policy and all other relevant policies.
- Making sure adequate procedures are implemented within their directorates or services to ensure compliance of these standards and all other relevant policies.

4.2. Managers

Managers are directly responsible for:
- The implementation of these standards and all other related SnowBe Online policies within the business areas for which they are responsible.
- Ensuring that all SnowBe Online employees who report to them are made aware of and are instructed to comply with these standards and all other relevant SnowBe Online policies.
- Consulting with the HR Department in relation to the appropriate procedures to follow when a breach of any of these standrds has occurred.

4.3. Network Domain Administrators

Each SnowBe Online network administrator is responsible for:
- Complying with these standandards and all other relevant SnowBe Online policies, procedures, regulations, and applicable legislation.
- Ensuring all passwords generated for new user accounts and password resets meet the requirements of these standards.
- Notifying users of their passwords in a secure and confidential manner.

4.4. System Administrators

Each SnowBe Online system administrator is responsible for:
- Complying with these standards and all other relevant SnowBe Online policies, procedures, regulations, and applicable legislation.
- Ensuring all passwords generated for new user accounts and password resets meet the requirements of these standards.
- Notifying users of their passwords in a secure and confidential manner.
- Complying with instructions issued by the IT Department on behalf of SnowBe Online.

4.5. System Developers

In addition, system developers, including both SnowBe Online personnel and third-party commercial service providers, are responsible for:
- Ensuring the systems and applications they develop for SnowBe Online are capable of implementing, supporting and enforcing these standards in full.

4.6. Users

Each user of SnowBe Online's IT resources is responsible for:

- Complying with these standards and all other relevant SnowBe Online policies, procedures, regulations, and applicable legislation.
- Respecting and protecting the privacy and confidentiality of the information systems and network they access, and the information processed by those systems or networks.
- Ensuring they only use user accounts and passwords which have been assigned to them.
- Ensuring all passwords assigned to them are always kept confidential and not shared with others including their co-workers or third parties.
- Changing their passwords at least every one hundred and twenty (120) days or when instructed to do so by designated system administrators, network domain administrators or the IT Department.
- Complying with instructions issued by designated information owners, system administrators, network administrators and/or the IT Department on behalf of SnowBe Online.
- Reporting all misuse and breaches of these standards to their manager.

5. Standards

PCS01 - Password Requirements

The following parameters indicate the minimum requirements for passwords for all individual accounts where passwords must be:

- A unique, combination of letters (both upper & lower case), numbers (0-9) and at least one special character (for example: “, £, $, %, ^, &, *, @, #, ?, !, €).
- A minimum of six (6) characters and a maximum sixteen (16) characters in length; If existing systems are not capable of supporting the minimum characters, then the maximum number of characters allowed within the system must be used.
- Not based on anything somebody else could easily guess or obtain using person-related information (e.g., names, SBOID, telephone numbers, dates of birth, etc.); and,
- Not vulnerable to a dictionary attack.
- Not re-used by a user within a twelve (12) month period.

PCS02 - Password Expiration

Most users are no longer required to change their passwords at fixed intervals. Some account types, such as privileged users, must still adhere to regular password changes. However, in all cases, the IT Department reserves the right to reset a user’s password in the event a compromise is suspected, reported, or confirmed. This helps prevent an attacker from making use of a password that may have been discovered or otherwise disclosed.

PCS02.1 - Standard Users

- Passwords must be changed upon suspicion or confirmation of compromise.
- New passwords must comply with the criteria in Section PSC01 - Password Requirements.

PCS02.2 - Privileged Users

- Privileged domain accounts must be stored in the Privileged Access Management (PAM) system and passwords rotated upon each use.

- Privileged accounts that cannot be stored in the PAM system must have their passwords changed every ninety (90) days.
- Passwords must not be reused for at least six (6) generations.
- Passwords must not be changed more than one (1) time per day.
- At least four (4) characters must be changed when new passwords are created.
- New passwords must comply with the criteria in Section PSC01 - Password Requirements.

PCS02.2 - Payment Card Industry (PCI) Users

- Passwords must be changed every ninety (90) days.
- Passwords must not be reused for at least four (4) generations.
- Passwords must not be changed more than one (1) time per day.
- At least four (4) characters must be changed when new passwords are created.
- New passwords must comply with the criteria in Section PSC01 - Password Requirements.

PCS02.3 - Service Accounts and Test Accounts

Passwords for service accounts and test accounts must be securely generated in accordance with these standards, distributed securely to the account owner, and stored securely in a password manager:

- Passwords must be changed upon suspicion or confirmation of compromise.
- Passwords must be changed when an account owner leaves the institution or transfers into a new role.
- Passwords must comply with the criteria in Section PSC01 - Password Requirements.

PCS03 - Account Lockout

In order to limit attempts at guessing passwords or compromising accounts, an account lockout policy is in effect for all systems. Account lockout thresholds and durations vary based on the type of user, as defined below.

PCS03.1 - Standard User Accounts

- Accounts will lockout after eighteen (18) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for a duration of fifteen (15) minutes, unless the IT Department is contacted, and the user's identity is verified in order for the account to be unlocked sooner.

PCS03.2 - Privileged User Accounts

- Accounts will lockout after eighteen (18) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for a duration of fifteen (15) minutes, unless the IT Department is contacted, and the user's identity is verified in order for the account to be unlocked sooner.

PCS03.2 - PCI User Accounts

- Accounts will lockout after six (6) invalid password attempts in fifteen (15) minutes.

- Accounts will remain locked for a duration of thirty (30) minutes, unless the IT Department is contacted, and the user's identity is verified in order for the account to be unlocked sooner.

PCS03.3 - Service and Test Accounts

- Accounts will lockout after two (2) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for a duration of thirty (30) minutes, unless the IT Department is contacted, and the user's identity is verified in order for the account to be unlocked sooner.

PCS03.4 - Mobile Device

- A mobile device will erase after ten (10) invalid password attempts.
- The IT Department can provide assistance in resetting device passcodes.

PCS04 - Mobile Devices

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

- Passwords must be at least six (6) digits.
- Passwords must not contain repeating or sequential digits (e.g., 111111, 123456, or 101010)
- Biometric authentication (e.g., facial or fingerprint recognition) on mobile devices may be used to unlock the device, but a compliant password must still be established.

PCS05 - Password Compliance Recommendations

In order to create a password that is compliant with the parameters specified in this policy, use one of the methods below.

PCS05.1 - Use a Passphrase

A passphrase is like a password, but it is generally longer and contains a sequence of words or other text to make the passphrase more memorable. A longer passphrase that is combined with a variety of character types is exponentially harder to breach than a shorter password. However, it is important to note that passphrases that are based on commonly referenced quotes, lyrics, or other sayings are easily guessable. While passphrases should not be famous quotes or phrases, they should also not be unique to you as this may make them more susceptible to compromise or password-guessing attacks.

- Choose a sentence, phrase, or a series of random, disjointed, and unrelated words.
- Use a phrase that is easy to remember.
- Passphrase Examples:
    - Password: When I was 5, I learned to ride a bike.
    - Password: fetch unsubtly unspoken haunt unopposed
    - Password: stack process overbid press
    - Password: agile stash perpetual creatable

PCS05.2 - Use a Secret Code

A secret code can be used in conjunction with the previous methods simply by substituting letters for other numbers or symbols. Combining these methods will make it easy to incorporate the four (4) character types in order to meet the password complexity

requirements.

- Use a phrase that is easy to remember
- Capitalize the first letter of every word
- Substitute letters for numbers or symbols
- Incorporate spaces or substitute with a different character
- Secret Code Example:
    - Phrase: “When I was five, I learned how to ride a bike.”
    - Password: WhenIwa$5,Ilh0wt0rab1k3.

PCS06 - Password Reset Options

Various options are available to assist users with changing a forgotten or expired password. The preferred and fastest method is through the use of the password management system. You must be enrolled in SnowBe Online’s Password Management System, Duo, and have a personal email address on file in order to use this system to reset your password. A department administrator or IT department agent may assist you with updating your personal email address, but you must provide proof of identity.

PCS06.1 - Password Self Service

You can change or reset your password in the myAccount system (https://identity.snowbeonline.com). If you know your current password and need to change it, click Change Password to authenticate with your current password and acknowledge a Duo push request. If you have forgotten your password, you will be required to validate your identity by verifying your personal email address and acknowledging a Duo push request.

In the event your password cannot be reset via the myAccount system, you must contact the IT Department using one of the methods below.

PCS06.1a - In Person

If you are working or visiting a SnowBe Online office:

- Visit the IT Department’s SMARTDesk during normal business hours.
- Present a valid identification card (must contain a photo), such as a driver license, passport, state identification, SnowBe Online identification, etc.) to verify your identity and supply a personal email address.
- Reset your password with the IT Department technician.

PCS06.1b - Remote

f you are unable to visit the SMARTDesk in person or use myAccount to perform a self-service reset, you may:

- Contact the IT Department during normal business hours and request to setup a video conference using Zoom with the agent.
- Conduct a video conference session with ITS Support if your computer or mobile device is equipped with a camera.
    - Present your valid photo identification card alongside your face to verify your identity.
    - The agent will assist with updating your personal email address and initiate the password reset process.

PCS07 - Reporting a Suspected Compromise or Breach
If you believe your password has been compromised or if you have been asked to provide your password to another individual, including the IT Department, promptly notify any of the following support teams within the IT Department:

- IT Security
  Phone: (555) 555-5550
  Email: it-security@it.snowbeonline.com

- IT Support
  Phone: (555) 555-5551
  Email: support@it.snowbeonline.com

- Privacy Office
  Phone: (555) 555-5552
  Email: privacy@it.snowbeonline.com

- SnowBe Online Hotline
  Phone: (555) 555-5552
  Online: http://hotline.snowbeonline.com

Filing or reporting a security incident can be done without fear or concern for retaliation.

6. Exemption

Exemption from certain procedure provisions may be sought by following the SnowBe Online's Exemption Process.

7. Enforcement

Any employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

8. Version History Table

Change Date	Version	Description	Document Owner	Approved By
09/24/2022	1.0	Working Draft of New Password Creation Standards	Samuel Oruh	Robin Groff Alarcon
Month/day/year				
Month/day/year				

9. References

HSE Password Standards Policy
https://www.hse.ie/eng/services/publications/pp/ict/password-standards-policy.pdf

Weill Cornell Medicine Information Technologies & Services
Password Policy and Guidelines
https://its.weill.cornell.edu/policies/1115-password-policy-and-guidelines