

SNOWBE ONLINE Policy# 25

Create a Password Procedure

Tyrall Waller

Group 6 Section 01

Draft - Version # 1.0

DATE: 3/29/25

Table of Contents

PURPOSE 2

SCOPE 2

DEFINITIONS 2

ROLES & RESPONSIBILITIES 2

POLICY & PROCEDURES 3

EXCEPTIONS/EXEMPTIONS 4

ENFORCEMENT 5

VERSION HISTORY TABLE 7

CITATIONS 8

Purpose

The purpose of this procedure is to provide the necessary steps to create, manage, secure and reset a password for SnowBe customers. The procedures provided have been created to ensure proper protection, storage and handling passwords and password protection.

Scope

The Create a Password procedure applies to all system users and employees who create, access, process, and handle informational data within the SnowBe business of operations. The established procedures for the enforcement of creating a password provide guidelines that ensure that all SnowBe personnel and all authorized access users adhere to the directed standards and utilization of resources.

Definitions

Sensitive data: Personal information which includes names, addresses, phone numbers, email addresses, credit card information and purchase history.

Encryption: The process of converting plaintext into ciphertext using a cryptographic algorithm and a key, making the information unreadable to anyone who does not have the appropriate key to decrypt the message.

Multi-factor Authentication: Multi-step process that requires users to enter More information as verification of identity to gain access to an account.

Roles & Responsibilities

Employees:

Must read, understand and adhere to the procedure that has been put in place to ensure passwords are secure and maintain confidentiality.

Information Technology Team:

Must read, understand and adhere to the procedure that has been put in place to ensure passwords are secure and maintain confidentiality.

Maintain the infrastructure, and implement all systems, firewalls and encryption protection.

Manage and audit new account access for accuracy of new account.

Audit system for access enforcement compliance within daily activity.

Have on-hand procedures for incident response for all incidents.

Security Team:

Must read, understand and adhere to the procedure that has been put in place to ensure passwords are secure and maintain confidentiality.

Provide scheduled security training to all hands.

Create, revise, maintain and cancel all policies and procedures.

Investigate and report all security and access incidents to higher authority with an after action report and follow-up action to resolve the related incident.

Monitor all activity to ensure all compliance regulations are being followed.

Identify, gather and analyze threat intel for possible risk or vulnerability.

Policy

The implementation of this procedure is to provide a step by step process to create, manage and recover a password. This procedure establishes standard procedure that define password requirement, creation, storage, communication, education and enforcement of what will successfully implement successful enforcement of passwords.

Procedures

Step 1: Creating a Password

Length: Aim for at least 12 characters, but longer is better.

Complexity: Use a mix of uppercase and lowercase letters, numbers, and symbols.

Uniqueness: Don't reuse passwords across multiple accounts.

Avoid: Personal information, common words, or easily guessable patterns.

Enter password, Reenter password and wait for confirmation for correct entry.

Step 2: Change a Password:

Find the Settings: Locate the "Security" or "Account" settings on the website or app.

Password Section: Navigate to the password management or security settings.

Enter Current Password: You'll likely need to enter your current password

to initiate the change.

New Password: Enter your new, strong password.

Confirm Password: Re-enter the new password to confirm.

Save Changes: Click "Save" or "Update" to finalize the password change.

Step 3: Store Passwords Securely:

Password Managers: Use a reputable password manager (e.g., LastPass, 1Password, Google Password Manager).

Encryption: Password managers store passwords securely using encryption.

Master Password: Choose a strong and unique master password for your password manager.

Avoid: Storing passwords in plain text or on insecure devices.

Step 4: Share Passwords Securely:

Use Password Managers: Password managers often have features for sharing passwords securely.

Secure Communication: Share passwords via encrypted channels (e.g., secure messaging apps).

Limit Access: Only share passwords with trusted individuals.

Password Legacy: If you have a password legacy, make sure to store it in a secure location and share it with the appropriate people.

Step 5: Recover a Password:

Forgot Password Link: Most websites and apps have a "Forgot Password" or "Reset Password" link.

Security Questions: You may be asked security questions to verify your identity.

Email or Phone Verification: You may receive a verification code or link via email or phone.

Password Reset: Follow the instructions to reset your password.

Recovery Information: Ensure you have access to your recovery email or phone number.

Exceptions/Exemptions

To ensure flexibility in security implementation while maintaining strong controls, the following exception/exemption policy applies:

1. Request Process:

a. Any request for an exception/exemption must be submitted in writing to the IT Security Manager.

b. The request must outline the reason, the systems affected, and the duration required.

2. Justification: The request must provide a valid business or operational reason that necessitates an exception.

3. Approved Authority: Approval must be granted by both the IT Manager and IT Director.

4. Duration:

a. Exceptions/exemptions will be granted for a limited period, subject to review every 6 months.

b. If an extension is required, a new request must be submitted along with the previous action provided.

Enforcement

A discharge by an employer of an individual for violation of an employer rule is for misconduct connected with the work if the rule is reasonable, the individual knew or should have known the rule, and the violation is willful or wanton, material, and substantially injures or tends to injure the employer's interests.

If the individual has previously violated a minor employer rule or has previously violated the same or a similar employer rule with the knowledge of the employer, a discharge is for misconduct connected with the work if the violation substantially injures or tends to injure the employer's interests and has been preceded by prior warnings or reprimands for previous violations, or if the individual's course of conduct as a whole demonstrates a substantial disregard of the employer's interests following prior warnings or reprimands for violations of other employer rules.

Thus, a violation of an employer rule is not, by itself, misconduct. It would be misconduct if all of the following conditions are met:

The rule is reasonable.

The claimant knew or should have known the rule.

The violation is willful and wanton.

NOTE: Violation of a reasonable employer rule is not willful if the claimant has shown good cause for violating the rule.

The violation is material.

The violation substantially injures or tends to injure the employer's interests. The employer has warned or reprimanded the claimant for previous violations of the same or similar employer rules.

Reasonable Rule

It is the employer's right generally to establish such rules for his or her employees as, in the employer's opinion, are necessary for the proper conduct of his or her business. Violation of an employer rule regarding the performance of the work will generally be a violation of a reasonable rule.

1. Knowledge of Rule

To be known, a rule must have been disseminated generally to all employees or made known to the claimant individually, either orally or in writing. If a claimant has been given a written copy of employer rules (as in an employee handbook), his or her failure to read the rules would not render the discharge for reasons other than misconduct. If the claimant was never informed of the existence of the employer rule, the discharge for violating the rule would generally not be for misconduct.

Some employer rules, however, do not need to be transmitted to the employee but are implied or are known rules in the occupation or industry. For example, there does not need to be a written employer rule against stealing of employer property or a formal employer rule that an employee in a bank does not drink on the job.

2. Violation is Willful

If a claimant has good cause for his or her violation of a rule, or if the violation is due to mere inefficiency, unsatisfactory conduct, failure in good performance as the result of inability or incapacity, inadvertence or ordinary negligence in isolated instances, or good faith errors in judgment or discretion, then there is no misconduct. Under such circumstances, the violation of the rule would not be a wilful, deliberate, or flagrant violation.

3. Materiality of Rule Violation

Violation of an employer rule is material when the employer's operations are interfered with.

4. Substantial Injury to Employer's Interest

From the definition of a "reasonable employer rule," it follows that any violation of a reasonable rule will injure or tend to injure the employer's interests. However, there is no misconduct unless the injury or tendency to injure is substantial.

5. Warnings and Reprimands

Some employer rules are such that their first violations would be misconduct, for example, rules prohibiting fighting or drinking on the job. Warnings and reprimands need not be considered for this kind of violations.

However, if the claimant has broken an employer rule which, although reasonable, is of comparatively slight significance, the claimant should be entitled to a warning or reprimand so that he or she would have the opportunity of mending ways before he or she was discharged. Therefore, if the employer has a rule about tardiness, or overstaying coffee-breaks, or any of the more minor conditions of employment, to constitute misconduct the employer would need to show that the claimant persisted in violating the rule despite warnings and/or reprimands.

What if the warnings or reprimands were not for the same type violations as the one which occasioned the claimant's discharge? Even so, the discharge would be for misconduct if the claimant's conduct, viewed in its entirety, evinced a deliberate disregard of the employer's interests. For example, a claimant may have been warned several times over a period of two or three months because of such violations as arguing with coworkers, wandering away from the workstation to engage in conversations, and failure to follow instructions. If, shortly after the last warning, the claimant violated an employer rule relative to tardiness by appearing at work 20 minutes late without good cause and was thereupon discharged, the discharge would be for misconduct.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	3/29/25	Tyrall Waller	Tyrall Waller	Create a Password Procedure

Citations

Create a Strong Password and a more secure account

(Google, 2025)

<https://support.google.com/accounts/answer/32040?hl=en>