



SNOWBE ONLINE

Create a Password Standard

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

STANDARD 3

EXCEPTIONS/EXEMPTIONS 4

ENFORCEMENT 5

VERSION HISTORY TABLE 7

CITATIONS 8

Purpose

The purpose of this standard is to provide the requirements for creating strong password utilization, protection for passwords and the frequency of how often the password should be changed.

Scope

The Create a Password Standard applies to all system users, which include employees, contractors, stakeholders, customers and third-party vendors and service providers who access SnowBe web applications and systems.

Definitions

Access Control: The process of managing who can access specific resources and what actions can be performed.

Approved Authorizations: Permissions granted to users or processes to access specific resources, based on their roles and responsibilities.

Logical Access: The ability to access information and system resources through a system's security mechanisms, such as authentication and authorization.

Multi-Factor Authentication: An additional security verification that is required to gain access to a network, system, website, account or application.

Password: A combination of characters used to authenticate a user's identity in order to grant user access.

Principle of Least Privilege: Users should only have access to the minimum level of privileges necessary to perform their job functions.

User Account: Collection of information and settings that enable a user to access a desired system. A username, password and additional user information all work systematically to identify the user, authenticate user access and provide the necessary permissions and access for the user to take action within the desired system.

Roles & Responsibilities

Employees:

Must read, understand and adhere to Password Standards that are put in place.

Contractors:

Adhere to all Password Standards.

Responsible for the implementation and maintenance of the security measures that protect all data and systems for Password Standards.

Ensure secure access enforcement in the monitoring and management of data by established guidelines and procedures.

Must fulfill all obligations agreed to, and previously established for the compliance of Password Standards.

Third-Party:

Adhere to all Password Standards.

Information Technology Team:

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

Manage user access and audit accounts for accuracy of active personnel and changes.

Audit system for password standard compliance within daily activity.

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

Security Team:

Adhere to all Password Standards.

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.

Standard:

The implementation of this standard enables system and data organization and the ability to create a process for password creation meeting required criteria in execution.

1. Length: Passwords must be no less than 8 characters.
2. Complexity: Passwords created will include a combination of the following:
 - Uppercase Letters
 - Lowercase Letters
 - Numbers
 - Special Characters
3. Personal Information: Passwords cannot use personal information, to include names, words, email, birthdays or common/known words.
4. Time: Passwords should be changed/updated within 120 Days or when compromised.
5. Multi-Factor Authentication: Multi-Factor Authentication must be implemented as part of creating the password in the beginning phase.
6. Password Recovery: The process to reset or recover passwords must be in place in the beginning phase.

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

Create a Password Standard – V 1.0

Status: ☒ Working Draft ☐ Approved ☐ Adopted

Document owner: Tyrall Waller

DATE 3/29/25

Citations

Information Security (Policy 9 – Password Policy)

(Murray State University, Feb 2011)

<https://sites.google.com/a/murraystate.edu/information-security/policy/password>