



SNOWBE ONLINE Policy# 2

Data Retention and Protection

Your name: Tyrall Waller

Group 6 Section 01

Draft - Version # 1.1

DATE: 3/9/25

Table of Contents

PURPOSE 2

SCOPE 2

DEFINITIONS 2

ROLES & RESPONSIBILITIES 2

POLICY 4

EXCEPTIONS/EXEMPTIONS 4

ENFORCEMENT 5

VERSION HISTORY TABLE 7

CITATIONS 8

Purpose

The purpose of this policy is to define, outline and manage retention periods, procedures, standards, guidelines and risks for SnowBe customer and business data, while ensuring security for sensitive and archived data, legal requirements, and resources are within compliance of industry regulations. This policy is also used to encrypt stored customer information, including purchase history and prevention of unauthorized access to data and data systems in case of a breach.

Scope

This Data Retention and Protection Policy applies to all users more specifically, departments, employees, contractors and third-party service providers to establish guidelines and procedures for the retention of data, outlining the retention and duration timeframe for data and stored data archiving methods. This policy ensures that all SnowBe personnel and all authorized access users adhere to the directed standards and utilization of resources.

Definitions

Information System: Hardware, Software, network, devices, and resources that processes data and information for the business purposes.

Data Retention and Disposal: Establish clear data retention policies ensuring legal compliance, contractual obligations and destruction of data methods are implemented. Retain all documentation of data, transactions, and audited logs for minimum of 1 year after the initial transaction date and implement a process to restore 6 months of data for analysis.

Protection of Records: (Create, Maintain, Store, and Dispose) Protecting the integrity and availability of physical and digital informational data from loss, damage, destruction, disaster and unauthorized access.

Data Encryption: Securing data by converting readable plaintext into an unreadable, encoded format.

Zero Trust Architecture: Security Architecture built to reduce an organization's attack surface, stop compromise, prevent lateral movement of threats, and block data loss in support of the organization's operational infrastructure.

Roles & Responsibilities

Employees:

Must read and understand the policies and procedures that are put in place.

Obligated to take ownership and responsibility by following established protocols in order to properly access, store and transmit the process of handling data in a secure manner.

Required to adhere to the directed security practice for login credentials, strong password and proper disposal of sensitive data guidelines.

Required to report unusual activity and possible and identified data breaches, and security incidents to the authorities and higher management.

Must comply with all relevant laws, regulations and internal policies related to data protection.

Contractors:

Adhere to all retention and data protection policies.

Responsible for the implementation and maintenance of the security measures that protect all data being handled.

Ensure secure transfer and storage of data by established guidelines and procedures.

Must fulfill all obligations agreed to, and previously established for security and compliance.

Third-Party:

Implement data security measures.

Outline data security obligation within all contracts.

Implement data sharing and data protection procedures.

Plan regular scheduled documented audits and assessments for current status of third-party risk and compliance.

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 equipment replacement, unusual activity and vulnerability.

Schedule regular backup and recovery procedures in order to implement, maintain and ensure data availability and protection.

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

Security Team:

Provide scheduled security training to all hands.

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

Investigate and report all security 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 policies, standard procedures, and guidelines enable the ability to manage, execute, protect and support all business activity and production in support of this organization and its infrastructure. By defining and managing data retention and protection with productive procedures put in place, this policy aims to produce nothing less the high quality effective management, retention, and data security while aiming to ensure legal requirement and compliance are being met as the end result.

Section leaders gather documented performance of data that drive action to make policy changes and decisions concerning data retention and data protection. Determination of retention scheduling, retention periods, expiration and review, archiving process, secure data deletion and personnel involvement are all the factors combined to create and implement a productive result.

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	3/9/25	Tyrall Waller	Tyrall Waller	Data Retention and Protection Policy

Citations

Data Retention and Archiving Policy

(Public Broadcasting Service, 2025)

<https://docs.pbs.org/space/DG/104792079/Data+Retention+and+Achieving+Policy>

Data Retention and Protection Policy: Roles and Responsibilities of Employees, Contractors, Third-Party, IT Team and Security Team

(Google AI Overview, 2025)

[data retention and protection policy: roles and responsibilities of employees, contractors, third-party, IT team and Security Team](#)

DRATA: What Is a Data Retention Policy? Best Practices + Template

(Tony Gagliardi, Nov 2023)

<https://drata.com/blog/data-retention-policy>

What is Zero Trust Architecture:

(ZSCALER, 2025)

<https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust-architecture>

Define Protection of Records

(Google AI Overview, 2025)

[define protection of records](#)

How do you shield data records from loss, destruction, falsification, unauthorized access, or release in alignment with legislative, regulatory, contractual and business obligations

(Google AI Overview, 2025)

[how do you shield data records from loss, destruction, falsification, unauthorized access or release in alignment with legislative, regulatory, contractual and business obligations](#)

Data Retention and Achieving Policy

(PBS, Sep 2024)

<https://docs.pbs.org/space/DG/104792079/Data+Retention+and+Achieving+Policy>