SNOWBE ONLINE
Policy# RM 2026-01
Risk Management

Group 2.2
Therasa Antoine
Version 1.0
Date 1/12/2026

Table of Contents

Purpose

The purpose of this policy is to establish a formal process for identifying, assessing, and mitigating information security risks. This policy is designed to protect SnowBe Online systems, customer data, and payment card information from unauthorized access, misuse, or compromise. It also ensures that the organization operates securely and remains compliant with applicable laws, regulations, and industry standards.

Scope

This policy applies to all individuals who access or use software, systems, or information within the SnowBe Network Database, including but not limited to internal systems, online platforms, cloud-based services, and third-party merchant environments. The risks addressed by this policy include operational risks, information system and data security risks, and risks associated with the processing, storage, or transmission of payment card data.

Definitions

Cloud services- Information resources i.e. software storage and computing power are handled by a third-party provider i.e. AWS.

Configuration - the set-up of hardware and software that completes the computer system

Analysis and Assessments – Test that ensure compatibility of all software while making sure all items are following the rules and regulations.

Roles & Responsibilities

IT Manager-Handles all IT issues and for all departments and management staff.

Technical Staff- maintaining all troubleshoot and security measures in for the entire personnel.

Employees and contractors to follow all rules and to report all incidents within a timely manner

Policy - The purpose of this policy is to establish a formal process for identifying, assessing, and mitigating information security risks to protect SnowBe Online's systems, customer data, and payment card information. This ensures the organization operates securely and complies with applicable regulations and standards.

Exceptions No exceptions will be granted unless supported by written documentation and approved in writing by two members of upper management. All exception requests must include complete documentation clearly justifying the necessity of the exception and the nature for why the exception is needed to benefit the business.

Enforcement This will begin with a verbal reprimand. If the behavior continues, a formal written warning will be issued, which will serve as the employee's first official counseling for the matter. The employee will then be required to undergo retraining on all company policies and procedures. If noncompliance persists after retraining, further disciplinary action will be taken in accordance with company policy such as suspension or subject to termination.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
RMA00-987	2026/01/12	antoine		

Citations

- https://secureframe.com/hub/nist-800-53/risk-assessment
- https://csf.tools/reference/nist-sp-800-53/r5/ra/ra-3/