SnowBe Incident Response Policy

Document Code: IR-1

Version: 1.0

Date: July 8, 2025

Author: Samantha Coleman

1. Purpose

The purpose of this policy is to establish a consistent approach for detecting, responding to, and recovering from information security incidents that affect SnowBe systems, data, and operations. A structured incident response helps limit damage, reduce recovery time, and protect the confidentiality, integrity, and availability of SnowBe's information assets.

2. Scope

This policy applies to all SnowBe personnel, systems, third-party vendors, and service providers that use or manage SnowBe's IT infrastructure, data, or services. It covers both confirmed and suspected security incidents, regardless of size or impact.

3. Roles and Responsibilities

- Incident Response Team (IRT) – Coordinates and manages response efforts, conducts root cause analysis, and documents the incident.
- IT Administrator – Assists in isolating affected systems, restoring services, and collecting forensic evidence.
- Department Heads – Ensure staff report incidents promptly and comply with response procedures.
- Employees and Users – Must report suspicious activity or incidents immediately to IT Security.

4. Definitions

- Security Incident: Anything that threatens the confidentiality, integrity, or availability of information and systems.
- Incident Response: An organized plan on how to handle security incidents effectively and efficiently.
- Containment: Actions taken to limit the spread or impact of an incident.
- Recovery: Steps to restore systems and data to normal operation.

5. Policy

- All employees must report any suspected or real security incidents immediately to the IT Security Team.

- SnowBe will maintain an Incident Response Plan that includes detection, analysis, containment, eradication, recovery, and post-incident review.
- The Incident Response Team must begin investigation within 1 hour of receiving a high-priority incident report.
- All incidents must be documented, including the timeline, actions taken, impact, and resolution steps.
- Containment efforts should prioritize limiting damage while preserving evidence for analysis.
- Recovery procedures must follow approved protocols to ensure system stability and data integrity.
- A root cause analysis and lessons learned review must be conducted after major incidents.
- Incidents involving customer or personal data breaches must be reported to compliance within 24 hours.