SNOWBE ONLINE Policy # SP-01: Patch Management Policy

James Chapman

<SP-01 Patch Management Policy>

Version # 1.0.0

Date 05/29/2025

Table of Contents

Introduction

The purpose of this policy is to establish a standardized approach for managing and applying security patches and updates to all SnowBe Online information systems. The goal is to reduce vulnerabilities, protect company assets, and ensure compliance with regulatory requirements by maintaining the confidentiality, integrity, and availability (CIA) of SnowBe Online's technology infrastructure.

Scope

This policy applies to all SnowBe Online employees, contractors, and third-party vendors who manage, access, or support company-owned or operated information systems, including servers, workstations, network devices, applications, and cloud services across all business units and geographic locations.

Definitions

- Patch: A software update intended to correct security vulnerabilities or improve system functionality.
- Vulnerability: A weakness in an information system that could be exploited to compromise system security.
- Critical Patch: A patch classified as high priority due to its potential to mitigate severe security risks.
- Patch Management: The process of identifying, acquiring, testing, and deploying patches to information systems.

Roles & Responsibilities

- Chief Information Security Officer (CISO): Oversees the patch management program and ensures compliance with this policy.
- IT Manager: Coordinates patch identification, testing, deployment, and documentation; conducts regular audits.
- System Administrators: Responsible for timely patch application, system monitoring, and reporting exceptions.
- Employees: Must report observed vulnerabilities and comply with scheduled maintenance notifications.
- Third-Party Vendors: Required to follow SnowBe Online's patch management standards for any systems or applications they manage

Policy

1. Patch Identification:
    - IT Manager and System Administrators must monitor vendor notifications and threat

intelligence feeds for new patches and vulnerabilities.
    - Critical patches must be identified within 24 hours of release.
2. Patch Assessment & Testing:
    - All patches must be evaluated for relevance and risk before deployment.
    - Patches must be tested in a controlled, non-production environment to ensure compatibility and stability.
3. Patch Deployment:
    - Critical security patches must be deployed to production systems within 72 hours of successful testing.
    - Non-critical patches must be applied within 30 days.
    - Emergency patches may be deployed immediately with expedited testing and approval.
4. Documentation:
    - All patching activities must be logged, including patch details, systems affected, testing outcomes, deployment dates, and responsible personnel.
    - Maintain a patch register for audit and compliance purposes.
5. Rollback Procedures:
    - A documented rollback plan must be in place for each patch deployment to restore systems in case of failure.
6. Exceptions:
    - If a patch cannot be applied, a risk assessment must be conducted, and compensating controls must be implemented.
    - All exceptions must be documented and approved by the CISO or IT Manager.

Exceptions/Exemptions

Requests for exceptions must be submitted in writing to the IT Manager, detailing the reason, affected systems, risk assessment, and proposed compensating controls. The IT Manager will review, assess, and approve or deny the request in consultation with the CISO. Approved exceptions must be reviewed periodically for continued validity.

Enforcement

Non-compliance with this policy may result in disciplinary action, up to and including termination of access or employment. The IT Security Compliance Team will monitor adherence and may escalate repeated or severe violations through formal enforcement actions, including mandatory remediation or revocation of system privileges.

Version History Table

Version	Date	Description
1.0	05/29/2025	First Draft of Patch Update Policy

Citations