SNOWBE ONLINE Policy# Software Patch Management Policy

Your name: Jedson Jerume

Software Patch Management

Policy- Version #

DATE:08/28/25

Table of Contents

Purpose

SnowBe relies on secure, reliable, and up-to-date technology to support its e-commerce platform, storefront operations, and business systems. Vendors regularly release feature updates, bug fixes, and security patches to enhance performance and eliminate vulnerabilities in their products. Timely adoption of these updates protects SnowBe's infrastructure—including AWS-hosted applications, point-of-sale systems, desktops, laptops, and servers—from threats, while also improving system stability, user experience, and overall productivity.

Unpatched systems expose customer data, financial information, and business operations to unacceptable risks. This Patch Management Policy:

- Defines expectations, requirements, and procedures for maintaining SnowBe systems and software.
- Establishes compliance reporting to verify patch management adherence.
- Outlines consequences for failing to comply with this policy.

Scope

This policy applies to all **SnowBe-owned systems, devices, and applications** that connect to the company's network, support business operations, or store customer and corporate data. This includes, but is not limited to, servers (on-premises and AWS-hosted), desktops, laptops, and point-of-sale (POS) systems used in SnowBe's U.S. and European storefronts, as well as devices in the Los Angeles headquarters.

SnowBe will maintain and track a formal inventory of systems and software subject to patch management, consistent with the **Asset Management Policy**. The inventory will be verified **quarterly** to ensure completeness and accuracy, allowing the IT team to properly assess all assets for patching and updating.

This policy covers the operating systems, applications, firewalls, antivirus solutions, backup servers, and remote monitoring and management (RMM) software deployed across SnowBe's infrastructure. At this time, employee-owned devices and Internet of Things (IoT) devices are not in scope for patching, and SnowBe acknowledges the risks associated with these exclusions.

Definitions

Asset Inventory: A documented list of all SnowBe-owned servers, desktops, laptops, POS systems, and applications that are subject to patching and updating.

Patch: A software update released by a vendor to fix vulnerabilities, correct errors, or improve performance.

Critical Patch: A vendor-issued update that addresses a high-risk vulnerability, such as one actively exploited by attackers or that could lead to significant data compromise.

Endpoint: Any device that connects to SnowBe's network, including desktops, laptops, and POS systems in storefronts.

Patch Management: The process of identifying, acquiring, testing, approving, and installing patches for systems and software in a timely manner.

Remote Monitoring and Management (RMM): Software deployed by SnowBe to monitor, manage, and update desktops, laptops, and servers remotely.

Zero-Day Vulnerability: A security flaw that is exploited by attackers before a vendor patch is available or before the organization can apply it.

Service Level Agreement (SLA): The agreed-upon timeframe in which patches must be tested and applied to SnowBe systems, based on the severity of the vulnerability.

Change Management: The structured process SnowBe follows to approve, schedule, and document updates or changes to its IT systems.

Unsupported Software: Any system, application, or version that no longer receives vendor patches or updates and poses a significant security risk.

Roles & Responsibilities

Project Manager (Karen): Oversees SnowBe's patch management program to ensure compliance with this policy. Coordinates with IT staff and management to align patching schedules with business needs and approves patch management reports for executive review.

IT & Cybersecurity Consultant (Brad): Provides expertise on patching processes and tools. Ensures RMM, antivirus, firewalls, servers, and endpoints are properly updated. Advises on prioritization of patches (critical vs. non-critical) and documents configurations for long-term operational continuity.

System Administrators / IT Staff:

Maintain the official asset inventory of SnowBe devices and systems.

Test patches before deployment to production systems when possible.

Apply operating system, application, and security patches within required timelines (e.g., 90 days for standard, immediately for critical/zero-day).

Monitor RMM dashboards and generate compliance reports.

Maintain documentation of patch status, testing, and remediation actions.

Storefront Managers:
Ensure POS terminals, desktops, and local equipment are available for patching and updates. Report issues or downtime caused by patch application to IT staff.

Employees (All Users):
Responsible for leaving devices powered on and connected during scheduled patch windows. Must not delay or bypass updates and should report any patch-related issues immediately to IT support.

Executive Management:
Reviews compliance reports, approves budget and resources for patch management, and enforces accountability for policy violations across the organization.

Policy

A. Patch Management Authority

The **Project Manager for IT Security** (currently Karen) is designated as the **Patch Management Authority** for SnowBe. This role holds the ultimate responsibility for planning, authorizing, and overseeing patch management activities. The authority may delegate execution tasks to IT staff, the cybersecurity consultant (Brad), or approved third-party vendors/tools (e.g., RMM).

The Patch Management Authority is responsible for verifying and approving:

- Patch Management Policy scope
- Patching priorities
- Patch testing and approvals
- Maintenance downtime for applying patches and updates
- Exceptions and mitigations for patches that cannot be applied
- Patch management reporting and enforcement

B. Patch and Update Acquisition

SnowBe's IT Department will continuously monitor vendors, security mailing lists, AWS alerts, and industry sources for patch notifications. Updates must be obtained directly from trusted vendors (e.g., Microsoft, AWS, firewall providers) or from approved service providers. Any patches from third-party sources must be carefully validated before use.

C. Patching Priority

If multiple patches are released, priority will be determined using:

- **CVSS score** (9.0–10.0 = Critical, 7.0–8.9 = High, 4.0–6.9 = Medium, 0.1–3.9 = Low)
- **Asset value** (e.g., AWS servers hosting e-commerce > office desktops)
- **Likelihood of exploitation** (reference CISA's exploited vulnerabilities list)

Each patch is scored from **2 (low priority)** to **30 (urgent action required)**. This ensures that patches for SnowBe's critical systems, such as credit card processing or customer databases, are prioritized above low-impact systems.

D. Patching and Update Schedule

Based on the priority score, SnowBe's IT Department will apply patches as follows:

- **24.0–30 (Critical):** Within 7 days
- **18.0–23.9 (High):** Within 14 days
- **Below 18.0 (Medium/Low):** Within 30 days
- **Non-security patches (bug fixes/upgrades):** Within 90 days

Servers and endpoints will generally be patched monthly, with **expedited patching for critical vulnerabilities**, especially those with known exploits.

E. Patching Guidelines

i. Patch Testing
High-value systems (AWS servers, AD, POS systems) may require testing in a controlled environment before deployment. Failed patches must follow the Exception and Mitigation process.

ii. Patch Preparation
Prior to applying patches, IT staff must ensure:

- Full system and data backups have been performed
- Rollback procedures are documented
- Backup hardware is available for critical systems (e.g., firewalls, servers)

iii. Automated Patch Management
Where supported, SnowBe will leverage **RMM tools, vendor automation, and built-in OS auto-updates**. Automated processes must only proceed after confirming backups and patch preparation steps.

iv. Manual Patch Management
For firmware, POS systems, or systems requiring downtime, IT must request approval from the Patch Management Authority. Requests should include affected systems, risk/urgency, proposed maintenance windows, and rollback plans. Emergency patches may be applied with executive approval or, if unavailable, at the IT Department's discretion with proper documentation.

v. Patch Verification and Testing
After applying updates, IT staff will verify that patches installed successfully and confirm that vulnerabilities are remediated. Any unsuccessful patches or persistent vulnerabilities must be documented and addressed under the Exception and Mitigation process.

Exceptions/Exemptions

Exceptions may occur in SnowBe's patching and updating process. These exceptions will be categorized as:

- **Failed Patches:** Updates that fail to install correctly on servers, desktops, laptops, or POS systems.
- **Disruptive Patches:** Updates that would cause unacceptable downtime for SnowBe's e-commerce platform, storefront operations, or business systems if applied immediately.
- **Unneeded Patches:** Non-security updates that add features not required for SnowBe operations. These will be recorded and re-evaluated quarterly.
- **Unpatched Vulnerabilities:** Certain assets (e.g., unsupported operating systems, legacy POS systems, or end-of-life vendor products) may remain unpatched due to vendor limitations.

All exceptions must be documented in SnowBe's **Exceptions List**.

For **Failed Patches, Disruptive Patches, and Unpatched Vulnerabilities**, mitigation is required. The IT Department, in coordination with Brad (Cybersecurity Consultant), will propose and implement mitigation strategies to reduce risks. Each plan must be approved by the **Patch Management Authority (Karen)** and include:

- Affected systems and their business role (e.g., AWS e-commerce server, POS terminal).
- Urgency of the vulnerability and potential impact.
- Proposed mitigation controls (e.g., firewall rules, access restrictions, segmentation, or enhanced monitoring).
- Preferred deployment timeframe, noting any required downtime.

The **Exception and Mitigation List** will be reviewed **quarterly** to:

1. Check if patches have since been released, allowing mitigations to be removed.
2. Confirm whether assets should be replaced, retired, or migrated (e.g., legacy servers).
3. Identify opportunities to improve existing mitigation strategies.

All quarterly reviews and mitigation decisions must be approved by the **Patch Management Authority**.

Enforcement

SnowBe is committed to maintaining a secure and compliant IT environment. Compliance with this Patch Management Policy is mandatory for all employees, contractors, IT staff, and third parties who manage or access SnowBe systems.

- **Employee Violations:** Any employee found intentionally violating this policy may be subject to disciplinary action, up to and including termination.
- **IT Staff Accountability:** The job performance of SnowBe's IT Department staff, including system administrators and consultants, will be evaluated in part or in full on their ability to meet patching requirements.
- **Negligence:** Regular failure to comply with patching requirements may be considered negligence. Falsified patch reports or gross negligence in execution may result in immediate disciplinary action or termination.
- **Non-Compliant Devices:** Devices (servers, desktops, laptops, POS systems, or IoT equipment) that do not meet patching requirements will be denied access to SnowBe's critical systems and data. Such devices may be restricted to a **segregated network or DMZ** until remediated and verified as compliant.

Enforcement of this policy ensures SnowBe reduces risk exposure, protects customer and corporate data, and maintains trust in its global operations.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
SP2.0	August 28th 2025	Jedson Jerume	Jedson Jerume	software patch management policy update

Citations

https://www.esecurityplanet.com/compliance/patch-management-policy-template/

https://www.roehampton.ac.uk/globalassets/documents/corporate-information/policies/cyber-security-policies/patch-management-policy.pdf/