SNOWBE ONLINE

Policy# PM01

Patch Management Policy

Chris Stevens

Software Patch Management

Version # 1.0

DATE: 10-28-2025

Software Patch Management – V 1.0
Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document owner: Chris Stevens
DATE: 10-28-2025

Table of Contents

Purpose

SnowBe Online's Patch Management Policy is to provide a framework for managing security vulnerabilities in all systems, applications, and network devices. This policy aims to protect the company's information systems and data from known exploits by ensuring that software and firmware patches are applied in a timely and systematic manner. This policy is critical for maintaining the confidentiality, integrity, and availability of SnowBe's IT infrastructure, including the AWS-hosted website, on-premise servers, and all end-user devices. It also supports the company's efforts to achieve compliance with regulatory standards like PCI.

Scope

This policy applies to all SnowBe Online employees, contractors, and third-party vendors who use, manage, or have access to the company's information systems and technology assets, including:

- All company-owned devices, including desktops, laptops, servers (on-premise and AWS), and mobile devices.
- All installed software, applications, and operating systems, including Windows, WordPress, and other vendor applications.
- All network infrastructure devices, including routers, switches, and firewalls.
- All systems and software that store, process, or transmit customer data, including credit card information, on the company's website database and storefront systems.

Definitions

Patch
A piece of software designed to fix problems or update a computer program or its supporting data.

Vulnerability
A weakness in a system that could be exploited by a threat.

Zero-day Vulnerability
A software vulnerability that has been disclosed publicly but is not yet patched.

Patch Management
The process of identifying, testing, and deploying patches to systems and software.

Roles & Responsibilities

IT Department
Responsible for the overall management and implementation of this policy. This includes identifying, testing, and deploying patches to all applicable systems and devices.

IT Director/IT Manager
Responsible for approving the patch management schedule, prioritizing critical patches, and granting exceptions to this policy.

Employees and Contractors

Responsible for cooperating with the IT department during patch deployment and ensuring their company-provided devices are connected to the network regularly for updates.

Enterprise IT Security

Responsible for reviewing and approving risk acceptance memos for non-compliance situations.

IT Information Systems

Responsible for reviewing risk acceptance memos.

Policy

All systems, applications, and network devices at SnowBe Online must be kept up-to-date with the latest security patches and updates.

Patch Identification

The IT Department will regularly monitor for security vulnerability announcements and new patches from vendors, including Microsoft for Windows servers and desktops, and AWS for the cloud platform.

Vulnerability Ranking and Prioritization

Patches will be ranked based on the severity of the vulnerability, potential impact on business operations, and exploitability. High-severity patches that address critical vulnerabilities will be prioritized for immediate deployment.

Testing

All major patches and updates will be tested in a controlled, non-production environment before deployment to the live production systems to ensure they do not introduce new issues or conflicts.

Deployment

Patches will be deployed according to a defined schedule. Critical and high-severity patches will be deployed within 48 hours of release, while medium- and low-severity patches will be deployed during scheduled maintenance windows.

Unpatched Systems

Systems that cannot be patched due to technical or business constraints must be formally documented and approved as exceptions. These systems should be isolated from the network or have additional compensating controls implemented to reduce risk.

Anti-Virus Updates

The IT Department will ensure that all anti-virus and anti-malware software is updated with the latest definitions on a daily basis.

Backup Software

The IT Department will ensure that all backup software is updated with the latest versions and patches as they become available to ensure data integrity and recoverability.

Firmware Updates

Firmware on all network devices, including routers and firewalls, must be updated regularly to address security vulnerabilities and improve performance.

Exceptions/Exemptions

Exceptions to this plan must be approved by the Information Security Office, under the guidance of SnowBe's IT Director and/or IT Manager. All exceptions will be formally documented. Plan exceptions will be reviewed on a periodic basis for appropriateness. Please note that while requesting exceptions or exemptions has been made available to you, it does not guarantee approval.

SnowBe Online recognizes that, under certain circumstances, deviations from this Acceptable Use Policy may be necessary to support specific business needs or technical requirements. Exceptions or exemptions to this policy may be granted under the following conditions:

Risk Acceptance
In some rare cases, a business case for non-compliance can be established. In all such cases, the non-compliance situation must be approved in advance through a risk acceptance process. This process requires a risk acceptance memo signed by a department manager and reviewed by IT Enterprise Security and IT Information Systems and approved by the IT Director and/or IT Management. Further details on the risk acceptance process can be obtained through the Enterprise IT Security Department.

Pre-Approval Required
All exceptions must be formally requested in writing and approved by the IT department and an authorized member of management. The request must clearly state the business justification, duration, and potential risks of the exception.

Documentation and Review
Approved exceptions will be documented and maintained by the IT department. All exceptions are subject to periodic review to ensure they remain valid and do not introduce unacceptable risks.

Temporary and Specific
Exceptions are granted on a temporary basis for clearly defined scopes and timeframes. They do not constitute a permanent change to the policy.

No Unauthorized Exceptions
Any deviation from this policy without documented approval is considered a violation and may result in disciplinary action, including suspension of access privileges.

Compliance Priority
Exceptions will not be approved if they compromise SnowBe Online's compliance with legal, regulatory, or security requirements.

Enforcement

Enforcement
SnowBe Online takes the enforcement of this (Policy name) seriously to protect its systems, data, and customers.

Violations of this policy, whether intentional or accidental, may result in disciplinary action, up to and including termination of employment, contract cancellation, and/or legal action.

The penalties will include the following components:

Monitoring and Auditing
SnowBe Online reserves the right to monitor, log, and audit all system and network activity to ensure compliance with this policy. Users should have no expectation of privacy when using company-owned systems or accessing company data.

Incident Investigation
Suspected policy violations will be investigated promptly by the IT department, Human Resources, and other relevant stakeholders. Users are expected to cooperate fully during any investigation.

Corrective Action
If a violation is confirmed, corrective actions will be taken based on the severity and nature of the breach. This may include revocation of access, mandatory training, written warnings, or other disciplinary measures as outlined in the employee handbook.

Legal Consequences
Activities that are illegal under local, state, or federal law may be reported to the appropriate authorities. This includes unauthorized access, data breaches, or misuse of customer financial information.

Appeals Process
Individuals who believe they were unfairly penalized for a policy violation may appeal the decision to management or HR following internal dispute resolution procedures.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	10-28-2025	Chris Stevens	CEO	Software Patch Management

Citations

Fordham University
https://www.fordham.edu/information-technology/it-security--assurance/it-policies-procedures-and-guidelines/patch-management-policy/
Policy, Purpose, Scope, Role & Responsibilities

Bowie State University
https://www.bowiestate.edu/files/resources/information-security-public.pdf
Exceptions/Exemptions

ChatGPT
https://chatgpt.com/c/681bc793-d1dc-800b-a676-cb7b3cf2678d
Exceptions/Exemptions, but as a group we revised the verbiage.

Policy Template
https://www.sans.org/information-security-policy/
Exceptions/Exemptions