SNOWBE ONLINE Policy# SI-02

Software Patch Management Policy

Humberto Gonzalez

Version # 1.0

DATE: November 5, 2024

Table of Contents

<Template Policy> – V 1.0
Status: ✠ Working Draft ☐ Approved ☐ Adopted
Document owner: Humberto Gonzalez
DATE: 11/23/2024

Purpose

This policy establishes a structure for managing software patches across SnowBe Online's systems in order to assure all software's security, functioning, and compliance, thereby preserving organizational assets and customer data.

Scope

This policy is applicable to all software and systems used by SnowBe Online. It includes workstations and laptops in the Los Angeles office, servers on-premises and hosted on AWS, the WordPress shopping cart platform used for online sales, and any third-party software integrated with SnowBe Online's business processes. It also includes VPN-connected laptops used for sales activity and any systems accessible through allowed mobile devices. This policy ensures that all detected vulnerabilities in these software systems are addressed quickly and efficiently using structured patch management techniques.

Definitions

Patch Management: The process of discovering, testing, and deploying updates to software, operating systems, and firmware in order to address vulnerabilities or improve functionality.

Non-Critical Patch: A software update that includes minor fixes or performance improvements.

PCI Compliance: Adhering to Payment Card Industry Data Security Standards.

Roles & Responsibilities

Employees:

- Use the systems as set by the IT department.
- Report any software-related difficulties right away.
- Follow all security protocols related to software use.

IT Department:

- Identify software and systems that require patches.
- Before deploying patches, ensure they are compatible and free of any concerns.
- Patches should be applied within the time limits specified.
- Monitor systems to ensure patch deployment is successful.
- Maintain records of patching activities and generate regular reports for senior management.

Senior Management/Executive Team:

- Allocate resources to support the patch management process.
- Support enforcement of the patch management policy.
- Patching reports should be reviewed to ensure that they are in line with business goals and regulatory requirements.

Third-Party Vendors:

- Provide timely updates about available fixes for SnowBe Online's software.
- Ensure fixes are applied in accordance with SnowBe Online's specifications.

Policy

1. Patch Identification: Conduct monthly vulnerability scans to detect software that requires patches, and subscribe to vendor notifications for critical and non-critical upgrades, including WordPress plugins and the shopping cart platform, for vulnerabilities.

2. Patch Testing: Test all patches in a controlled environment before deploying to production systems to ensure compatibility, performance stability, and compliance with PCI DSS standards.

3. Patch Prioritization: Critical patches must be applied within 7 days after their identification or distribution by the vendor, whereas non-critical patches must be applied within 30 days.

4. Patch Deployment: Deploy patches to production systems only after successful testing, and use automated tools whenever possible to ensure correct and timely patching across SnowBe Online’s on-premises and AWS-hosted systems.

5. Verification and Monitoring: Verify patch deployment to ensure successful implementation, and monitor patched systems for stability and performance.

6. Documentation and Reporting: Keep track of all patches applied, including patch IDs, dates, and affected systems, and provide monthly reports for management review. Systems that handle credit card data must document compliance with PCI DSS rules as part of this reporting.

Exceptions/Exemptions

In circumstances where regular security standards cannot be followed, exceptions or exemptions may be requested. To request an exception or exemption, the requester must send a formal written request to the IT department, outlining the precise security protocol that cannot be followed and the justification for the request. The request should include a reason for why the exception or exemption is required, the potential impact on security, and any proposed compensatory controls. The Chief Information Officer (CIO) or a designated senior IT executive has the power to approve or reject such requests. Approved exceptions or prohibitions will be provided for a brief period not exceeding one year unless otherwise justified. The requester must make certain that the exception or exemption is reviewed and re-evaluated before the end of the permitted term.

Enforcement

All SnowBe Online employees, contractors, and third-party entities must comply with this security policy. Failure to follow the policies and procedures outlined will result in disciplinary action, which may include verbal or written warnings for minor infractions, temporary suspension from duty for repeated or serious violations, and termination of employment for severe or repeated noncompliance. If noncompliance results in legal consequences or financial loss for SnowBe Online, the company has the right to take legal action. Contractors and third-party entities that violate this security strategy may face contract termination and legal action, depending on the severity of the breach. All disciplinary actions will be carried out under SnowBe Online policy and any applicable labor laws. Each individual must understand and follow security policies to protect the company's information assets.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	11/23/2024	Humberto Gonzalez	TBD	The Initial version of the Software Patch Management Policy.

Citations

Exceptions/Exemptions- Sample Detailed Security Policy (bowiestate.edu)

Patch management- Patch Management Policy Template

Purpose/Introduction- Michigan Technological University Information Security Plan (mtu.edu)

Software Patch Management- Cybersecurity and Privacy Reference Tool | CSRC

Roles & Responsibilities- Sample Detailed Security Policy (bowiestate.edu)

Enforcement- Sample Detailed Security Policy (bowiestate.edu)