SNOWBE ONLINE Policy#02 System and Software Patch Management

Your name: Paola Baez Hernadez

< Policy#02 System and Software Patch Management **> - Version #02**

DATE: 05-29-2025

Table of Contents

Purpose

The purpose of this policy is to ensure all software, systems, and devices at SnowBe Online are updated in a timely and secure manner to reduce vulnerability to cyber threats and maintain operational integrity.

Scope

This policy applies to all SnowBe Online-managed hardware, operating systems, software applications, and cloud services.

Definitions

Critical Patch: A security update addressing a vulnerability with a high risk of exploitation.

Patch: A software update designed to fix vulnerabilities, improve functionality, or enhance performance.

Patch Window: A scheduled timeframe during which patches are tested and deployed.

Roles & Responsibilities

- **IT Department:** Manages patch schedules, testing, deployment, and monitoring.
- **Security Team:** Determines patch priorities based on risk and validates successful application.
- **System Owners:** Confirm systems operate correctly after patches are applied.

Policy

1. **Patch Evaluation:** Weekly scans must identify outdated or vulnerable software.
2. **Patch Priority:**
    - **Critical patches:** Apply within 7 days.
    - **High-severity patches:** Apply within 14 days.
    - **Others:** Address during monthly updates.
3. **Testing & Backup:** Patches must be tested in staging before deployment; full system backups must be verified.

4. **Automation:** Anti-virus and firmware updates should be automated where feasible.

5. **Documentation:** All patching activities must be recorded, including success/failure status.

Exceptions/Exemptions

Any deviations from this policy must be submitted for review and approval by the IT Director or CISO. Documentation must include a business justification and mitigation plan.

● To ensure compliance with internal standards, exceptions or exemptions requests are handled through a specific procedure. These requests are reviewed, justified, and approved according to SnowBe Online's internal guidelines.
● The dropdown for submitting Exceptions/Exemptions requests can be found on the SnowBe Online associate portal webpage. Allowing staff members to easily request exceptions or exemptions from regular rules and processes, guaranteeing that any deviations are appropriately recorded and examined.

● The request form is available through the “Compliance Forms” tab, located at the top right of the page. This ensures consistency throughout the process; this centralized location makes it simple for employees to find, be able to view, and send requests.
● The form for requesting exceptions or exemptions is titled “Exceptions/Exemptions” within the drop-down window. This clearly labels the form for exception or exemption requests, ensuring that the process is straightforward, and users can identify the correct form to address their specific needs.

● Requests for exceptions or exemptions are made when deviations from standard procedures or policies are necessary due to specific circumstances, such as operational needs, technical constraints, or temporary situations. Any changes are carefully thought through and examined before they are accepted as a result of these requests.

Approval Hierarchy:

● IT: The IT Director or IT Manager will perform the initial review to ensure the requested exemption does not compromise SnowBe Online's security, infrastructure, or compliance.
● Management: Management will review the request to confirm alignment with business objectives and ensure that no critical operations are disrupted.

● Final Authority: The IT Director or IT Manager holds the final authority on all exceptions or exemptions, ensuring decisions align with SnowBe Online’s overall business strategy, security requirements, and compliance obligations.

Approval Notification: Once the request is submitted, the requester will receive an email notification indicating whether the request was approved or denied. The status of the request can also be tracked via the SnowBe Online associate portal webpage.

Enforcement

Systems found to be out of compliance may be temporarily removed from the network. Repeated violations may lead to disciplinary actions.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
V2.0	05-29-2025	Paola Baez		Initial Patch Management policy release

Citations

https://www.pwc.com/us/en/technology/alliances/microsoft/cybersec
urity.html?WT.mc_id=CT3-PL300-DM1-TR1-BR_SA_-OTHERBM_-
Microsoft_Google_Search&gclsrc=aw.ds&gad_source=1&gad_cam
paignid=15454933137&gclid=Cj0KCQjwucDBBhDxARIsANqFdr2f9
0TiUqRezPkvuDQHX2Pjq7NvtPUVa_m5PGJyYQJ_APLvfYbpSEIa
Ah-3EALw_wcB