Patch Management Policy

SnowBe Corporation

Version 1.0

Date: March 30, 2025

Contents

1 Introduction

The purpose of this policy is to ensure that all organization-owned devices are proactively managed and patched with appropriate security updates. In addition, this policy is intended to instruct and inform the SnowBe community about the change in endpoint computing.

2 Scope

This policy applies to all Enterprise Servers which are owned by the organization. It also applies to SnowBe-issued Windows endpoints bound to Active Directory (AD).

3 Definitions

- **Scheduling and Deployment:** Software vendors release security patches on a regular schedule. Applicable patches will be tested and validated by Information Services (IS) prior to deployment to campus. Once validated, IS will schedule and deploy validated patches to endpoints monthly. Communication to campus regarding deployed security patches will be done through Pilots announcements.
- **Installation and Validation:** A system reboot is required to successfully install most security patches. Until the reboot occurs, the computer remains vulnerable to attacks which the installed patch protects against. IS understands the impact an ill-timed reboot can have on user productivity. In order to provide the SnowBe community with as much flexibility as possible, security updates will be deployed using an "optional-mandatory" method. The optional-mandatory method will allow users to install scheduled updates at their convenience before a deadline occurs. Users will be provided five (5) business days to select the installation time of their choosing for deployed patches. After the deadline passes, updates will automatically install and may enforce reboots of the computer as the updates require. It is strongly recommended that users install the updates as soon as possible to ensure that endpoints are protected and rebooting does not disrupt work. When updates are available, a notification will appear in the system tray. The message will continue to appear daily until the updates are installed and will appear more frequently as the deadline approaches.
- **Out-of-Band Updates:** On occasion, a software vendor will release a highly critical security patch outside of their normal release cycle. The usual reason for the release of an out-of-band patch is the appearance of an unexpected, widespread, destructive exploit that will likely affect a large number of users. In the event of a published out-of-band patch, Information Services (IS) will expedite the validation process. Once validated, users will have two (2) business days to install and reboot their machine to apply the patch. After the deadline passes, updates will automatically install and may enforce reboots of your computer as the updates require. IS will communicate to the campus via Pilots announcements in the event of an out-of-band update deployment.
- **Mandatory Reboot Exemption:** There is the possibility of academic or administrative processes being negatively impacted even with a five-day window for users to apply patches. Users who could be impacted in this scenario may contact the SnowBe Helpdesk and re-

quest to be temporarily exempted from the mandatory reboot process. The endpoints being exempted will still have patches deployed regularly, but it will be the responsibility of the end user to reboot the machine to apply those security patches. Each request will be reviewed on a case-by-case basis and will have a limited duration for exemption.

4 Roles & Responsibilities

- **Business Unit Directors:** Ensure that their staff maintain knowledge of patch releases either through subscribing to the appropriate mailing list or by direct notification from the vendor.
- **System Administrators:** Enter a change ticket according to the change management policy when a patch is announced. Assign a criticality rating of either high or normal, based on vendor information or their experience if no criticality is supplied.
- **Security Analyst:** Perform a vulnerability scan on the systems after each patch window to show that the patches were installed correctly. Submit clean vulnerability scan reports to the Infrastructure Manager quarterly for review.
- **Information Services (IS):** Responsible for testing, validating, and deploying patches, as well as communicating updates via Pilots announcements.

5 Statement of Policies, Standards, and Procedures

SnowBe Online is committed to ensuring a secure computing environment and recognizes the need to prevent and manage IT vulnerabilities. A compromised computer threatens the integrity of the network and all computers connected to it. Patch and vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. Proactive management of vulnerabilities will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after exploitation has occurred. All servers under Information Services (IS) control will be maintained with the latest security patches to their operating systems and key applications.

1. Each business unit is responsible for devices and systems under their control.
2. Business unit directors must ensure that their staff maintain knowledge of patch releases either through subscribing to the appropriate mailing list or by direct notification from the vendor.
3. When a patch is announced, an authorized system administrator must enter a change ticket according to the change management policy.
4. When the ticket is entered, a criticality rating of either high or normal must be assigned. Criticality ratings are usually supplied by vendors, but in the case that no criticality is supplied, the system administrator must assign a rating based on his/her experience.
5. All high/critical patches must be applied as soon as practically possible, but no longer than thirty (30) calendar days after public release for any critical production server.
6. All patches that are medium/high severity or for non-critical systems must be rolled out

within ninety (90) calendar days.

7. Any low priority patches will be installed on a case-by-case basis. All patches should be tested on development systems before being rolled out to production, where possible.
8. In the case where patches cannot follow the schedule, a document must be produced explaining why the patch must be deferred. Permissible deferrals may include a lack of appropriate change windows within the appropriate timeframe or a conflict with other critical changes scheduled at that time.
9. Any patches which are to be deferred longer than the scheduled timeframe must be approved by the Chief Information Officer (CIO) or his/her assignee. All deferred patches must be reviewed at least quarterly.
10. All patches for vendor-maintained systems/applications that are labeled as high/critical and apply to security must also be patched within 90 days of the approved release from the vendor.
11. Any functional but non-critical patches may be installed on a case-by-case basis. IS is responsible for maintaining knowledge of these patches and ensuring that vendors comply with our internal policy.
12. The Security Analyst is responsible for performing a vulnerability scan on the systems after each patch window to show that the patches were installed correctly. Clean vulnerability scan reports should be submitted to the Infrastructure Manager quarterly for review.
13. All SnowBe-owned Windows-based endpoints are to have critical operating system and key application patches installed within 30 days of release from the vendor.

6 Exceptions/Exemptions

Exceptions must be approved by the Chief Information Officer (CIO). There are no other exceptions for this policy.

7 Version History

Version	Date	Author	Description
1.0	March 30, 2025	SnowBe Policy Team	Initial policy draft

Table 1: Version History

8 Citations

- University of Portland. (n.d.). Patch management policy. `https://www.up.edu/is/files/policypatchmanagement.pdf`