,

SNOWBE ONLINE

Policy SP-14

Patch Management Policy

Daphnie Bruno

SP-14 - Version # 1.0

March 24 2025

Table of Contents

Purpose

The purpose of this policy is to enforce patch requirements for SnowBe Online-owned or managed IT Resources.

Scope

This IT policy, and all policies referenced herein, shall apply to all members of SnowBe Online, including administrative officials, staff, authorized guests, delegates, and independent contractors (the "User(s)" or "you") who use, access, or otherwise employ, locally or remotely, the SnowBe Online IT Resources, whether individually controlled, shared, stand-alone, or networked.

Definitions

IT Resources include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

A patch is a software update comprised of code inserted (i.e., patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package. Patches include, but are not limited to, the following:

- Updating software
- Fixing a software bug
- Installing new drivers
- Addressing new security vulnerabilities
- Addressing software stability issues

Patch management cycle is a part of lifecycle management and is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.

Roles & Responsibilities

Chief Information Security Officer (CISO):

- **Leadership and Oversight:** The CISO leads the Information Security and Assurance (ISA) office, overseeing the development and implementation of the University's information security program, which includes patch management strategies.
- **Policy Approval:** The CISO is responsible for approving security policies, ensuring they align with the University's strategic objectives and compliance requirements.

Information Technology (IT) Department:

- **Implementation and Maintenance:** The IT department is tasked with implementing and maintaining the technical aspects of patch management, ensuring that all IT resources are up-to-date with the latest security patches.
- **Resource Allocation:** IT managers must ensure that sufficient financial, personnel, and other resources are available to support technological business continuity and disaster recovery plans, which include patch management activities.

Development Teams:

- **Secure Coding Practices:** Development teams are responsible for adhering to secure coding practices and integrating security measures, such as timely patching, into the software development lifecycle to mitigate vulnerabilities.
- **Documentation and Testing:** They must document all development phases and conduct thorough testing to ensure that patches do not introduce new vulnerabilities or disrupt existing systems.

Security Team:

- **Risk Assessment and Mitigation:** The security team conducts risk assessments to identify vulnerabilities and collaborates with other departments to implement appropriate patches and remediation strategies.
- **Monitoring and Compliance:** They continuously monitor IT resources for compliance with security policies and the effectiveness of applied patches, ensuring the integrity and availability of systems.

Employees (General Faculty, Staff, and Students):

- **Compliance with Policies:** All employees are required to comply with the University's IT policies, including adhering to guidelines related to patch management to maintain the security of IT resources.
- **Incident Reporting:** Employees must promptly report any security incidents or potential vulnerabilities to the appropriate authorities to facilitate timely remediation.

Policy

- All IT Resources must be part of a patch management cycle.
- Owners and managers are responsible for the assessment of IT Resources under their management or supervision.
- All patches or configuration changes must be deployed to SnowBe Online-owned or managed IT Resources when a vulnerability is determined per the Vulnerability Management Policy.

Exceptions/Exemptions

Any exceptions to this policy must be documented and approved by the Chief Information Security Officer (CISO). Exceptions may be granted only for business-critical needs where compliance with this policy would significantly hinder operational performance, provided there is an alternative security mitigation in place.

Enforcement

Violations of this Security Maturity Policy will result in disciplinary actions, which may include, but are not limited to, verbal or written warnings, suspension, termination of employment, or legal action, depending on the severity of the violation.

- 1st violation, verbal coaching.
- 2nd violation, written coaching.
- 3rd violation, associate retraining.
- 4th violation, suspension.
- 5th violation, termination.

Regular audits and monitoring will be conducted to ensure compliance, and employees are encouraged to report any suspected security incidents or policy breaches to the IT Security team immediately. IT audits will be conducted monthly at discretion of the IT manager. The senior IT Manager will summarize the audit findings monthly and present it to the CISO.

Version History Table

Version #	Implementation Date	Document Owner	Approved By	Description
1.0	March 24, 2025	Daphnie Bruno		Created Patch Management Policy

Citations

- Grammarly, Inc. (n.d.). *Grammarly: Free writing assistant*. Retrieved from https://www.grammarly.com Used to correct grammar errors and spelling errors.
- **NIST**: National Institute of Standards and Technology. (n.d.). *NIST Cybersecurity Framework*. Retrieved from https://www.nist.gov/cyberframework
- Patch Management Policy – Fordham University: