Status: ☒ Working Draft ☐ Approved ☐ Adopted
Document owner: Thomas Ayres
Implementation Date: 11/20/2022

Software Patch Management Policy

V1.0

THOMAS AYRES

Purpose

Software must be patched across all systems and applications for various reasons. This policy is in place to guide that process a bit.

Scope

Patch management policies within enterprise environments cover a wide range of information and operational technology (IT/OT) assets, systems, and applications, including the following:

- device endpoint operating systems
- server operating systems
- IoT firmware
- operational technologies
- virtualization platforms
- network and device peripherals
- network components
- applications
- databases
- storage platforms
- unified communications systems
- IT management and monitoring tools

Definitions

Patch – an update to an application that usually fixes vulnerabilities found in the current version.

Roles & Responsibilities

N/A

Policy

A. GENERAL

All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. System components and devices attached to the SnowBe Online network shall be regularly maintained by applying critical security patches within thirty (30) days after release by the vendor. Other patches not designated as critical by the vendor shall be applied on a normal maintenance schedule as defined by normal systems maintenance and support operating procedures.

B. SYSTEM, UTILITY AND APPLICATION PATCHING

A regular schedule shall be developed for security patching of all SnowBe Online systems and devices. Patching shall include updates to all operating systems as well as office productivity software, data base software, third party applications (e.g. Flash, Shockwave, etc.), and mobile devices under the direct management of SnowBe Online IT Department.
Most vendors have automated patching procedures for their individual applications. There are a number of third-party tools to assist in the patching process and SnowBe Online should make use of appropriate management software to support this process across the many different platforms and devices the SnowBe Online IT supports. The regular application of critical security patches is reviewed as part of normal change management and audit procedures.

C. PATCHING EXCEPTIONS

Patches on production systems (e.g. servers and enterprise applications) may require complex testing and installation procedures. In certain cases, risk mitigation rather than patching may be preferable. The risk mitigation alternative selected should be determined through an outage risk to exposure comparison. The reason for any departure from the above standard and alternative protection measures taken shall be documented in writing for devices storing non-public data. Deviations from normal patch schedules shall require [Insert Appropriate Role] authorization.

D. SECURITY PATCHING PROCEDURES

Policies and procedures shall be established and implemented for vulnerability and patch management. The process shall ensure that application, system, and network device vulnerabilities are:

- Evaluated regularly and responded to in a timely fashion
- Documented and well understood by support staff
- Automated and regularly monitored wherever possible
- Executed in a manner applicable vendor-supplied tools on a regularly communicated schedule
- Applied in a timely and orderly manner based on criticality and applicability of patches and enhancements

[ref.1]

Exceptions/Exemptions

N/A

Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.
[ref.1]

References

[1] *Data Privacy and Security*. CDE. (n.d.). Retrieved November 20, 2022, from https://www.cde.state.co.us/dataprivacyandsecurity

Version History

Version Number	Change Date	Document Owner	Approved By	Description
0.1	9/5/22	Thomas Ayres		Initial Template
1.0	11/20/22	Thomas Ayres		Initial Policy