SecOps® Solution

# Vulnerability Patch Management

**Free Use Disclaimer:** *This policy may be utilized entirely or in part by your organization without restriction. There is no need for prior authorization. Please email hello@secopsolution.com if you would like to contribute a new policy or an updated version of this one.*

## 1. Overview

Patch Management at **<Company Name>** is required to mitigate risk to the confidential data and the integrity of **<Company Name>**'s systems.

Patch management is an effective tool used to protect against vulnerabilities, a process that must be done routinely, and should be as all-encompassing as possible to be most effective.

**<Company Name>** must prioritize its assets and protect the most critical ones first; however, it is important to ensure patching takes place on all machines.

## 2. Purpose

This policy's objective is to specify vulnerability patch management policy inside **<Company Name>**. It aims to ensure vulnerabilities are managed according to the risk in the **<Company Name>**.

Given the number of computer workstations and servers that comprise the **<Company Name>** network, it is necessary to utilize a comprehensive patch management solution that can effectively distribute security patches when they are made available. Effective security is a team effort involving the participation and support of every **<Company Name>** employee and the Board of Directors.

## 3. Scope

It ensures that all vulnerability patch management is done by the employee or professional appointed by the **<Company Name>**. And the results obtained after patch management are kept confidential and distribution of results outside the company is prohibited unless approved by the Company.

## 4. Policy

**4.1** Vulnerability:

a. The ISO is authorized to conduct routine scans of devices, systems, and applications connected to **<Company Name>** to identify operating system and application vulnerabilities.

b. All Information System Owners are required to ensure routine initiation and review of the results of vulnerability scans of devices, systems, and applications for which they are responsible and to evaluate, test, and mitigate, where appropriate, identified vulnerabilities.

c. Vulnerability scanning and review must be repeated as part of each annual risk assessment conducted pursuant to the Information Security Risk Management and Security Planning Policy, as well as each time a change is made that may introduce additional vulnerabilities. Information System Owners must coordinate with the infosec to schedule these scans and ensure a timely (as determined by risk) review of findings.

**4.2** Patch Management

a. The infosec must produce and maintain a Patch Management Standard that defines the minimum information security standards necessary to ensure the protection of **<Company Name>** and Information Resources. The minimum standards must include the following requirements:

1. A risk-informed systems patch cycle for all server operating systems (OS) must be scheduled, as appropriate, for Information Systems and related subsystems.
2. Any emergency patching outside of the routine patching schedule must be done according to the level of risk, as determined by the Information System Owner in consultation with the ISO.
3. Servers, services, or applications must be maintained with current OS, application, or security patch levels, as recommended by the software manufacturer and informed by risk, to protect **<Company Name>** Information from known information security issues.

b. All Information System Owners must ensure the implementation of processes and procedures that provide assurance of compliance with the minimum standards produced by the ISO.

## 5. Policy Compliance

**5.1 Compliance Measurement:** The ISO must develop, test, review, maintains, and communicate a representation of the **<Company Name>** information security posture to **<Company Name>** leadership. The ISO is authorized to initiate mechanisms to track the effective implementation of information security controls associated with this policy and to produce reports measuring individual or Unit compliance to support **<Company Name>** decision-making.

**5.2 Exceptions:** Requests for exceptions any to information security policies may be granted for Information Systems with compensating controls in place to mitigate risk. Any requests must be submitted to the CISO for review and approval pursuant to the exception procedures published by the CISO

**5.3 Non-Compliance:** The ISO is authorized to limit network access for individuals or Units, not in compliance with all information security policies and related procedures. In cases where **<Company Name>** resources are actively threatened, the CISO must act in the best interest of the **<Company Name>** by securing the resources in a manner consistent with the Information Security Incident Response Plan. In an urgent situation requiring immediate action, the CISO is authorized to disconnect affected individuals or Units from the network. In cases of noncompliance with this policy, the **<Company Name>** may apply appropriate employee sanctions or administrative actions, in accordance with relevant administrative, academic, and employment policies.

## 6. Definition and Terms

**ISO:** The University's Information Security Office, is responsible for coordinating the development and dissemination of information security policies, standards, and guidelines for the University.

**Vulnerability:** Any weakness in a system or process that leaves information security exposed to a threat.

## 7. Revision History

| Version | Date | Description |
|---|---|---|
| 1.0 | 17-01-2023 | Initial Policy |