# [INSERT FIRM LEGAL NAME]
# Patch Management Policy

**[Insert Firm Logo]**

**Version 1.0**
**[Insert Date]**

**This document is proprietary and confidential. The document and information contained herein may not be shared outside of [Insert Firm Legal Name] unless approved by authorized personnel.**

## Contents

## Instructions

**Documents are in a template format and are to be customized to fit the appropriate business and operational requirements.** Use the sample as a foundation to build a bespoke policy for your business.

If any element of the following Sample/Template is not operationally feasible or appropriate for a particular business, be sure to delete that element from the company-specific document. **Otherwise, it would be a liability exposure to establish a policy and not to comply with it.**

The following recommendations are designed to limit, but will not eliminate, the security risks associated with the use of the policy subject. Businesses should deploy a defense-in-depth security model of technical, operational, and physical security controls.

**Delete the instructions after finalizing and adopting the policy.**

**This document is enhanced using Human Intelligence (Hi) from the Riskigy vCISO team. For additional tuning and generating bespoke policies, procedures and plans the team can be reached at info@riskigy.com**

## Policy Overview

Passwords are an important aspect of computer security. Passwords must be chosen and secured from this point forward with the highest possible degree of care and attention. Passwords are critical to user account access which includes firewall administration, email and web access, and full disk backup for  A poorly chosen password may result in the compromise of the organization’s entire corporate network. As such, all employees or volunteers/directors (including contractors and vendors with access to systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Patch Management Policy is a guide to patching software vulnerabilities in operating systems, Web browsers, and other iconic applications that are used by businesses. The security risks posed by these flaws can be significant, so it’s essential for organizations to develop effective patch management programs that ensure the timely application of critical security patches.

Vulnerabilities within a computer system can be exploited by unauthorized users, which may result in the compromise of confidential company data. The security team will monitor vendor websites for released updates, and deliver patch notifications to development.

Patches, which are security related or critical in nature, should be installed as soon as possible.

In the event that a security or critical patch cannot be centrally deployed, it must be installed in a timely manner using the best resources available.

This policy requires that all workstations are properly configured to install approved patches/updates on an automated schedule. Failure to comply with this policy is a violation of company policy and can lead to financial penalties or prosecution through the company's legal department.

**Responsibilities**

Patch management is one of the central components of the information security program. The VP of IT is responsible for ensuring that all computers and networking devices are running at their highest security level. It is the organization’s policy to ensure that all computer devices connected to the network have the most recent operating system and application patches installed.

The use of computing and network resources is a privilege, not a right. All users are required to adhere to the policy governing their respective use of computing and network resources, regardless of whether they are acting in a professional or personal capacity.

IT is responsible for ensuring all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. These defenses include patching, firewalls, antivirus systems, and intrusion detection mechanisms.

IT Management and Administrators will coordinate with each other to review vendor notifications and websites, and research specific public websites for the release of new patches. In addition, monitoring will include but is not limited to:

- ➢ Network scanning is a vital part of any complete network security program. It is used to identify vulnerabilities in the environment and protect against known threats. Scheduled third-party scanning of the network occurs, using the most up-to-date security patches and software.
- ➢ The Vulnerability Management program is designed to provide an organization with a comprehensive understanding of the security landscape and be able to remediate identified vulnerabilities.
- ➢ This policy describes the standards and procedures for monitoring security vulnerabilities and patches for servers, network devices, and appliances. The objective of this policy is to reduce the risk to information and physical assets while improving critical business services by monitoring events that could impact the organization.

- ➢ The IT Security and System Administrators are responsible for maintaining the accuracy of patching procedures to ensure the documents are current and up to date. This includes a detailed description of the what, where, when, and how to eliminate confusion in the day-to-day operations which enables routine auditing of these practices.
- ➢ Patch Management Policy is to protect the confidentiality, integrity, and availability of the information system that is being used within the organization. Patching involves making software code changes from multiple sources into one code base. Each patch will fix a specific issue within the system and allow it to continue running smoothly. This is done by configuring the network infrastructure and server environment in order to run applications safely and securely while increasing productivity by improving the performance, reliability, and flexibility of its data center operations.
- ➢ Once alerted to a new patch, IT Administrators will download and review the new patch. The patch will be categorized by criticality to assess the impact and determine the installation schedule. Critical patches are installed immediately. Non-critical patches are scheduled for installation at a later time but within 30 days of release. It is important that all users update their operating systems in order to protect their information from malicious attacks.

## Scope and Purpose

**Scope**

This patch management policy applies to all employees and consultants, such as all electronic devices, servers, application software, computers, peripherals, routers, and switches. The goal of this policy is to ensure that all systems in the environment are kept up-to-date with the latest security patches and security versions.

**Purpose**

The goal of the Patch Management Policy is to protect the integrity of our infrastructure, systems, and data by maintaining our software and hardware at the most current available version. In order to accomplish this, we will utilize a comprehensive patch management solution that can effectively distribute security patches. Effective security involves the participation and support of every employee.

## Compliance

The Information Security team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

**Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Exceptions

Any exception to the policy must be approved by the Information Security team in advance.

## Appendix

None

## Revision Table

| **Revision History** | | | | |
|---|---|---|---|---|
| **#** | **Version #** | **Date** | **Updates/Changes** | **Owner** |
| **1** | 1.0 | 2023 | Initial Draft | Riskigy |
| **2** | | | | |