# **A close-up of a logo  Description automatically generated**

# **Patch Management Policy**

## Overview

Regular installation of vendor-issued critical security updates and patches is necessary to protect [COMPANY] data and systems from malicious attacks, performance problems and errors. All electronic devices connected to the network including servers, workstations, firewalls, network switches and routers, tablets, mobile devices, and cellular devices, as well as operating system software and applications routinely require patching to maintain secure business operations and performance.

## Purpose

Software is critical to the delivery of services to [COMPANY] customers and internal users. This policy prescribes a continuous and consistent process for regular security updates and patches to operating systems, firmware, software applications and utilities. Regular updates are critical to maintaining a secure and well-performing operational environment.

## Scope

This policy applies to all [COMPANY] employees and contractors who create, deploy or support IT infrastructure, devices and software. Oversight and enforcement of the policy shall be the responsibility of the [COMPANY][TITLE].

## Policy

### GENERAL

The [TITLE] or delegated staff shall create an inventory of IT assets that should fall under the purview of this policy. All identified assets shall be protected from known vulnerabilities by installing applicable vendor-supplied security patches. The [TITLE] or delegated staff will rank available patches by criticality. Patches deemed critical will first be tested in a controlled environment to identify potential business disruptions and other risks. Patches that fail may be omitted from deployment as long as the procedures for patching exceptions (below) are followed.

System components and devices attached to the [COMPANY] network shall be regularly maintained by applying critical security patches within [NUMBER] days of release by the vendor. Other patches not designated as critical by the vendor or [TITLE] shall be applied on the normal maintenance schedule defined in [COMPANY] systems maintenance and support procedures.

A comprehensive backup of systems and data should be executed before an update or patch is applied. Critical systems, such as servers and routers, might require redundant infrastructure that can be put on standby in case an update causes system failure. There should be a rollback procedure for restoring systems to a prior state in the event of such a failure.

Systems and applications shall be monitored to verify that a patch was installed and did not introduce new issues, and that the security vulnerabilities or bugs to be addressed by the patch have been removed or that new features are operational.

### SYSTEM, UTILITY AND APPLICATION PATCHING

A regular schedule shall be developed for security patching of all [COMPANY] systems and software. Patching shall include updates to all operating systems as well as business applications, database software, utilities, network infrastructure, hardware, firmware and mobile devices under the direct management of [COMPANY][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 [COMPANY] should make use of appropriate patch management software to support this process across the different platforms, networks and devices the [COMPANY] [DEPARTMENT] supports. However, some IT assets require manual updating, which the automated patching providers should identify in advance.

Regular application of critical security patches, bug fixes and feature updates will be reviewed as part of the organization's change management and auditing procedures.

### PATCHING EXCEPTIONS

Patches on production systems (e.g. servers and enterprise applications) might require complex testing and installation procedures. In certain cases, risk mitigation rather than patching might be preferable. Risk mitigation steps should be determined by comparing the risks of an outage to the security and compliance risks. The reasons for departing from the above standards, as well as alternative protection measures taken, shall be documented in writing for devices storing non-public data. Deviations from normal patch schedules shall require prior authorization from the [TITLE].

### D. PATCHING PROCEDURES

Additional policies and procedures may be established and implemented for vulnerability management and patch management. They should 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
* Regularly monitored
* Mitigated in a timely and orderly manner based on the criticality and applicability of patches and feature enhancements

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this policy as part of [COMPANY] internal systems change management and update procedures. Examples of adequate controls include the following:

* Documented change management meetings and conversations between key [COMPANY] stakeholders.
* System updates and patch logs for all major hardware, software and network categories.
* Logs including system ID, date patched, patch status, exception and reason for exception.
* Demonstrated infrastructure supporting enterprise patch management across systems, applications, and devices.

## Enforcement

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

## Distribution

This policy is to be distributed to all [COMPANY] executives and to staff responsible for IT support and management as defined in the scope.

## 8. Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
|  |  |  |  |
|  |  |  |  |

 Sources: Colorado Department of Education, Heimdal, TechTarget