

# Managed IT & Patch Management

Endpoint Updates • Server Maintenance • Operational Security

Patch Management

Windows/Linux Systems

WordPress Updates

Network Devices

## Overview

This public sample shows how EPIC TECH LLC frames patch management as an ongoing operational security process rather than a one-time update task.

## Business Challenge

Unpatched endpoints, servers, VPN-connected laptops, web platforms, and network devices can expose businesses to avoidable attacks and downtime.

## Example Solution

A patch management model was created with severity-based timelines, owner responsibilities, testing expectations, documentation, exception handling, and verification requirements.

## Technologies / Methods Demonstrated

- Patch Management
- Windows/Linux Systems
- WordPress Updates
- Network Devices
- AWS Systems
- Change Control
- Compliance Evidence

## Business Outcomes

- Improved update accountability.
- Prioritized critical and high-risk fixes.
- Created audit-friendly records for maintenance and compliance.

## What This Shows a Client

- Shows managed IT operations capability.
- Shows practical security maintenance knowledge.
- Shows ability to create repeatable service processes.

## Details intentionally not published

- Full internal update schedules.
- Specific client systems.

- Administrative procedures.
- Exception records and internal approvals.

This document is designed to give website visitors confidence in EPIC TECH LLC capability without publishing full implementation playbooks or reusable client deliverables.