Pragmatic GRC™

C-008
Patch Management Policy Guide

Cybersecurity Operations Resource | Version 1.0 | Practical Implementation Guide

Executive Summary

Effective patch management reduces the likelihood of successful cyberattacks by ensuring operating systems, applications, firmware, and network devices receive timely security updates. This guide provides a practical, risk-based patch management approach for SMBs.

Document Information

Field	Value
Resource ID	C-008
Resource Family	Cybersecurity Operations
Version	1.0
Related Chapters	4, 8
Related Resources	F-001, F-002, R-001, C-002, G-002

1. Purpose

Establish a standardized process for identifying, evaluating, testing, approving, deploying, and verifying software and firmware patches.

2. Scope

Applies to servers, workstations, laptops, cloud services, mobile devices, network infrastructure, virtual machines, and business applications.

3. Roles and Responsibilities

Define responsibilities for executive leadership, system owners, IT/MSPs, application owners, and business stakeholders.

4. Patch Classification

Classify updates as Emergency, Critical, High, Medium, or Routine based on vendor severity and business risk.

5. Patch Management Lifecycle

Inventory assets, identify updates, assess risk, test patches, obtain approvals, deploy updates, verify successful installation, document exceptions.

6. Recommended Patch Timeframes

Emergency: 24 hours; Critical: 7 days; High: 14 days; Medium: 30 days; Routine: 60–90 days, based on business needs.

7. Exception Management

Document approved exceptions, compensating controls, business justification, owner, expiration date, and review frequency.

8. Metrics and Reporting

Track patch compliance, overdue systems, failed deployments, emergency patches, and exception counts. Review results during the Monthly GRC Heartbeat™.

9. Integration with Pragmatic GRC™

Update the Master Asset Register (F-001), Unified System Security Plan (F-002), and Enterprise Risk Register (R-001) whenever significant patching risks or exceptions are identified.

Patch Management Workflow

Maintain Asset Inventory (F-001)
↓
Identify Available Patches
↓
Assess Risk & Priority
↓
Test Updates
↓
Deploy Patches
↓
Verify Installation

↓
Document Exceptions
↓
Review During Monthly GRC Heartbeat™

Recommended Patch Priorities

Priority	Target Deployment	Examples
Emergency	Within 24 Hours	Actively exploited vulnerabilities
Critical	Within 7 Days	Remote code execution
High	Within 14 Days	Privilege escalation
Medium	Within 30 Days	Security improvements
Routine	60–90 Days	Feature updates

Best Practices

- Maintain an accurate asset inventory.
- Test critical patches before broad deployment.
- Document emergency changes and exceptions.
- Verify successful installation after deployment.
- Review patch metrics during the Monthly GRC Heartbeat™.

Revision History

Version	Date	Author	Description
1.0		Pragmatic GRC™	Initial publication