Patch Management Policy

Version: 1.0

Status: Approved

Applies to: All employees, contractors, and service providers

Last Reviewed: (Insert Date)

---

1. Purpose

The purpose of this Patch Management Policy is to ensure that all information systems and software applications are kept up to date with the latest vendor patches, updates, and security fixes. This policy reduces exposure to cyber threats, system compromise, and operational disruption.

This policy supports compliance with:

- ISO 27001 (A.12.6.1, A.14.2.3)
- NIST Cybersecurity Framework (PR.IP-12)
- CIS Controls v8 (Control 7 & 4)
- Regulatory and contractual obligations

---

2. Scope

This policy applies to:

- All operating systems
- Workstations, laptops, servers, virtual machines
- Network devices (firewalls, switches, routers)
- Cloud environments (AWS, Azure, GCP, M365)
- Third-party and internally developed applications
- Mobile devices managed by the organisation
- Employees, contractors, and vendors responsible for system maintenance

---

3. Policy Objectives

The objectives of this policy are to:

1. Reduce system vulnerabilities by applying updates promptly
2. Identify missing patches and configuration weaknesses
3. Prioritise patching based on risk and exploitability
4. Maintain a consistent patch cycle

5. Verify patch installation success
6. Improve the overall security posture of the organisation

---

4. Roles and Responsibilities

4.1 IT/Security Team

- Monitor vendor patch releases
- Review Microsoft Patch Tuesday updates
- Maintain patch automation tools (Intune, WSUS, RMM, etc.)
- Test patches in pilot groups
- Deploy patches according to timelines
- Report patch compliance and failures

4.2 System/Application Owners

- Approve changes related to patching
- Report operational issues caused by updates
- Ensure third-party applications remain supported

4.3 Management

- Approve risk acceptance requests
- Review patch compliance reports
- Provide resources necessary for patch management

4.4 Third-Party Providers

- Patch hosted systems not directly controlled by the organisation
- Provide patch compliance status on request

---

5. Patch Identification

Patches must be identified from:

- Vendor security bulletins
- OS update channels (Windows Update, Linux repos)
- Cloud security services (Azure Defender, AWS Inspector)
- Threat intelligence (CISA KEV, MSRC)
- Vulnerability scan results
- Application vendor notifications

Automatic monitoring tools should be reviewed daily or weekly.

---

6. Patch Classification

Patches are classified based on severity:

Severity	Description	Examples
Critical	Actively exploited or high-risk vulnerabilities	Zero-days, RCE flaws
High	High likelihood exploit, major impact	Privilege escalation
Medium	Moderate impact	Local vulnerabilities
Low	Minor impact	Cosmetic fixes

---

7. Remediation Timelines

The following timelines apply unless superseded by regulatory requirements:

Severity	Timeline
Critical	**24–72 hours**
High	**≤ 7 days**
Medium	**≤ 30 days**
Low	**≤ 90 days**

Exceptions must be approved by management using the Risk Acceptance Form.

---

8. Patch Deployment Process

1. Identify new patches
2. Evaluate severity and business impact
3. Test patches in a controlled environment
4. Schedule deployment (maintenance window when appropriate)
5. Deploy patches through automation or manual installation
6. Reboot systems as required
7. Verify installation success
8. Conduct follow-up scans

Deployment tools may include:

- Microsoft Intune
- WSUS
- RMM systems
- Linux package managers (apt/yum/dnf)
- Vendor-specific tools (VMware, Cisco, etc.)

9. Testing and Validation

Before deployment:

- Critical systems must undergo testing in a staging/pilot environment
- Compatibility issues must be documented
- Rollback procedures must be defined
- Backups must be validated

If a patch causes issues, it must be escalated to system owners.

10. Patch Compliance Monitoring

Patch performance must be measured monthly and include:

- Compliance percentage (endpoints and servers)
- MTTR: Mean Time To Remediate
- Failure rate
- Recurrent missing patches
- Overdue critical or high-severity items

Dashboards must be maintained via Intune, WSUS, or custom reporting tools.

11. Exceptions and Risk Acceptance

Exceptions are permitted only when:

- A patch breaks business functionality
- A system cannot be updated without vendor intervention
- A machine is end-of-life and awaiting replacement

Exceptions must:

- Be documented using the Risk Acceptance Form
- Include justification, compensating controls, and expiry date
- Be approved by management

12. Enforcement

Non-compliance with this policy may result in disciplinary action.

Repeated failures to patch critical systems may trigger:

- Access restrictions
- Managed isolation of devices
- Escalation to senior leadership

---

13. Definitions

Patch: A vendor-supplied fix for vulnerabilities or defects

Zero-day: A vulnerability actively exploited before a patch is available

CVSS: Industry-standard scoring system for vulnerabilities

KEV: CISA Known Exploited Vulnerabilities

MTTR: Mean Time To Remediate

---

14. Document Control

Version	Date	Author	Notes
1.0	(Insert Date)	(Insert Name)	Initial release