Vulnerability Management Policy

Version: 1.0

Status: Approved

Applies to: All staff, contractors, service providers

Last Reviewed: (Insert date)

---

1. Purpose

The purpose of this Vulnerability Management Policy is to ensure that all systems, applications, and services within the organisation are routinely scanned, assessed, and remediated for security vulnerabilities in a timely and risk-based manner.

This policy supports:

- Protection of confidentiality, integrity, and availability
- Compliance with ISO 27001, NIST CSF, CIS Controls v8
- Reduction of cybersecurity exposure
- Alignment with regulatory and contractual obligations

---

2. Scope

This policy applies to:

- All production and non-production systems
- Servers, endpoints, network devices
- Cloud systems (AWS, Azure, GCP, M365)
- Third-party hosted services
- Custom-developed applications
- Staff, contractors, and vendors involved in system management

---

3. Policy Objectives

The key objectives of this policy are to:

1. Identify vulnerabilities through scanning, monitoring, testing, and intelligence sources
2. Assess vulnerabilities using a consistent risk methodology

3. Prioritise remediation based on business impact and exploitability
4. Apply patches and mitigating controls within defined timelines
5. Track, report, and verify vulnerability remediation
6. Reduce attack surface and improve overall security posture

---

4. Roles and Responsibilities

4.1 IT/Security Team

- Conduct regular vulnerability scans
- Analyse results and assign risk scores
- Apply patches and mitigating controls
- Report metrics and compliance rates
- Ensure tools are up-to-date

4.2 System/Application Owners

- Approve remediation actions
- Validate that fixes do not break business operations
- Participate in risk acceptance where required

4.3 Management

- Review vulnerability dashboards
- Approve exceptions and risk acceptance
- Ensure adequate resources are available

4.4 Third-Party Vendors

- Ensure hosted systems are patched
- Provide patch compliance reports on request
- Maintain secure configurations

---

5. Vulnerability Identification

The organisation will identify vulnerabilities using:

- Authenticated vulnerability scans
- External perimeter scans
- Cloud security tools (e.g., Azure Defender, AWS Inspector)
- Vendor security bulletins
- CISA Known Exploited Vulnerabilities (KEV) list

- Threat intelligence feeds
- Penetration testing and code reviews
- Application security assessments

---

6. Risk Scoring and Prioritisation

Vulnerabilities will be assessed using a combined model:

- **CVSS Score**
- **Business Impact**
- **Exploitability**
- **Criticality of system**
- **Exposure (internal vs external)**

Remediation Timelines:

Severity	Description	Timeline
Critical (CVSS 9.0–10)	Actively exploited / high impact	**24–72 hours**
High (CVSS 7.0–8.9)	High likelihood of compromise	**≤ 7 days**
Medium (CVSS 4.0–6.9)	Moderate impact vulnerabilities	**≤ 30 days**
Low (CVSS 0.1–3.9)	Minor exposures and misconfigurations	**≤ 90 days**

Exceptions must be documented and approved by management.

---

7. Remediation and Patching Process

1. IT team reviews vulnerability scan results
2. Vulnerabilities triaged by severity and business impact
3. Patching team tests updates in a controlled environment
4. Rollout via automated tools (Intune, WSUS, RMM, etc.)
5. Change control applied for significant updates
6. Reboot and verification
7. Follow-up scan confirms remediation

Remediation may include:

- Installing vendor patches
- Updating software versions
- Disabling vulnerable features
- Configuration hardening
- Compensating controls if patching is not possible

---

8. Vulnerability Exceptions & Risk Acceptance

When patches cannot be applied within defined timelines due to business constraints:

- A formal **Risk Acceptance Form** must be completed
- Approval must come from **Management or the DPO**
- Compensating controls must be implemented
- Exceptions must have an expiry date
- Residual risks must be documented

---

9. Verification & Reporting

9.1 Verification

- Follow-up scans confirm vulnerabilities are remediated
- Logs must show successful patch installation
- Critical vulnerabilities require evidence of fix

9.2 Reporting Requirements

Weekly/Monthly reports must include:

- Total vulnerabilities
- Critical/High open vulnerabilities
- Average MTTR (Mean Time to Remediate)
- Patch compliance percentage
- Repeat offenders (assets frequently missing patches)
- Exceptions and overdue risks

---

10. Continuous Improvement

The organisation will:

- Review vulnerability metrics quarterly
- Conduct annual penetration testing
- Update tooling based on industry best practices
- Adjust remediation timelines as needed
- Document lessons learned

---

11. Enforcement

Non-compliance with this policy may result in:

- Disciplinary action
- Removal of system access
- Reporting to regulatory authorities for repeated failures

---

12. Definitions

Vulnerability: A weakness in a system that could be exploited.

Patch: A vendor-supplied software fix.

CVSS: Common Vulnerability Scoring System.

MTTR: Mean Time to Remediate.

---

13. References

- ISO 27001: A.12.6 & A.14.2
- NIST Cybersecurity Framework (PR.IP-12, DE.CM)
- CIS Controls v8 (Control 7 & 4)
- CISA KEV Catalogue

---

14. Document Control

Version	Date	Author	Changes
1.0	(Insert)	(You)	Initial Release