System Security Policy Document

System Security Policy

Document Title: Vulnerability Management and Asset Discovery Policy

Version: 1.0

Approved By: CISO

Effective Date: 2025-05-01

Review Cycle: Annually

1. Purpose

To ensure the security of all IT assets and online services by establishing clear guidelines for asset discovery, vulnerability scanning, and timely patch management in compliance with the Australian Information Security Manual (ISM) controls.

2. Scope

This policy applies to all IT infrastructure, systems, cloud environments, and applications operated or managed by the company, including production, development, and testing environments.

3. Policy Statements

3.1 Automated Asset Discovery

- The company must use an automated asset discovery tool across all networks at least once every fortnight (14 days).
- This tool must be capable of identifying new, removed, or modified assets, including:
  - Endpoints
  - Servers (on-premises and cloud-hosted)

  - Network devices
  - Software applications
- All identified assets are to be logged in the company's IT Asset Register and automatically forwarded to the Vulnerability Management System.

ISM Alignment: Control requires fortnightly automated discovery for accurate and ongoing visibility of assets.

3.2 Vulnerability Scanning

- The company must conduct vulnerability scans on all discovered assets using a vulnerability scanner with an up-to-date vulnerability database.
- Vulnerability scanning must occur at least weekly, and after any significant change to infrastructure or software.
- The vulnerability scanner must be updated daily with the latest CVEs, exploit signatures, and vendor advisories.
- Scanning must include authenticated (credentialed) scans wherever possible for improved coverage.

ISM Alignment: Ensures missing patches and exposed configurations are detected using current vulnerability intelligence.

3.3 Patch and Mitigation Management

- All critical vulnerabilities, as defined by the vendor or where working exploits exist, must be remediated within 48 hours of the vendor release.
- Criticality assessment is based on:
  - Vendor severity rating (e.g., CVSS 9.0+)
  - Exploitation in the wild (as confirmed by threat intel feeds)

- Remediation includes:
  - Patch application
  - Configuration changes
  - Disabling vulnerable components or applying workarounds
- Non-critical vulnerabilities must be addressed based on risk assessment and business impact.

ISM Alignment: Requires timely action (within 48 hours) for high-risk vulnerabilities affecting online services.

4. Roles and Responsibilities

Role	Responsibility
IT Operations Team	Run asset discovery scans, maintain inventory
Security Team	Schedule and analyze vulnerability scans, initiate remediation
System Owners	Approve and implement patches or mitigations
CISO	Ensure policy compliance and reporting to executive management

5. Monitoring and Reporting

- Asset discovery and vulnerability scanning logs must be retained for at least 12 months.
- Weekly reports must be submitted to the Security Operations Center (SOC) including:
  - Number of discovered assets
  - Detected vulnerabilities and severity
  - Remediation status and timeline compliance

6. Non-Compliance

Failure to comply with this policy may result in disciplinary action, audit findings, or increased risk exposure and must be reported to the CISO.

7. Policy Review

This policy shall be reviewed annually or after any major changes to IT infrastructure or ISM requirements.