Vulnerability Management Policy

Organization: AegisCISO
Document ID: POL-VULN-001
Version: 1.0
Effective Date: January 2026
Classification: Internal
Owner: Chief Information Security Officer (CISO)

---

1. Purpose

This policy establishes the framework for identifying, assessing, prioritizing, and remediating security vulnerabilities in AegisCISO systems to reduce the attack surface and protect information assets.

2. Scope

This policy applies to:

- All information systems and applications
- All network devices and infrastructure
- All cloud resources
- All endpoints and mobile devices
- All personnel responsible for system security

3. Vulnerability Identification

3.1 Vulnerability Scanning

POL-VULN-001-01: Regular vulnerability scanning shall be conducted.

Asset Type	Scan Frequency	Scan Type
External-facing systems	Weekly	Authenticated + Unauthenticated
Internal servers	Monthly	Authenticated
Workstations	Monthly	Authenticated
Network devices	Monthly	Authenticated
Cloud resources	Weekly	API + Agent-based
Web applications	Weekly	DAST
Containers/Images	Every build + Weekly	Image scanning

3.2 Scanning Tools

POL-VULN-001-02: Approved vulnerability scanning tools.

Requirements:

- Enterprise vulnerability scanner for infrastructure
- Web application scanner (DAST)
- Static application security testing (SAST)

- Container image scanner
- Cloud security posture management (CSPM)
- Tools maintained with current vulnerability databases

3.3 Scanning Coverage

POL-VULN-001-03: Scanning coverage requirements.

Requirements:

- All IP addresses in scope
- All web applications covered
- Credentials for authenticated scans
- Scan exclusions documented and approved
- Coverage metrics tracked (target: 100%)

3.4 Threat Intelligence

POL-VULN-001-04: Threat intelligence integration.

Requirements:

- Subscribe to vulnerability advisories (NVD, vendor, CERT)
- Monitor for zero-day announcements
- Correlate with threat intelligence feeds
- Prioritize based on active exploitation

4. Vulnerability Assessment

4.1 Severity Classification

POL-VULN-001-05: Vulnerabilities shall be classified by severity.

Base Classification (CVSS):

Severity	CVSS Score	Description
Critical	9.0 - 10.0	Immediate exploitation risk
High	7.0 - 8.9	Significant risk if exploited
Medium	4.0 - 6.9	Moderate risk
Low	0.1 - 3.9	Limited risk

4.2 Risk-Based Prioritization

POL-VULN-001-06: Vulnerabilities shall be prioritized based on risk.

Prioritization Factors:

- CVSS base score
- Asset criticality (Tier 1-4)
- Exploit availability
- Network exposure (external vs internal)
- Compensating controls

- Business context

Risk Priority Formula:

```
Priority = (
```

4.3 False Positive Management

POL-VULN-001-07: False positives shall be managed.

Requirements:

- Validation before marking as false positive
- Documentation of validation method
- Approval for false positive status
- Periodic review of false positives
- Tuning of scan policies

5. Vulnerability Remediation

5.1 Remediation Timelines

POL-VULN-001-08: Remediation SLAs based on risk priority.

Risk Priority	Remediation Timeline	Escalation
Critical	72 hours	CISO at 48 hours
High	7 days	Security Manager at 5 days
Medium	30 days	Team Lead at 21 days
Low	90 days	Quarterly review

5.2 Remediation Methods

POL-VULN-001-09: Approved remediation methods.

In order of preference:

1. Patch/Update: Apply vendor security patch
2. Upgrade: Upgrade to non-vulnerable version
3. Configuration Change: Modify settings to eliminate vulnerability
4. Compensating Control: Implement alternative protection
5. Accept Risk: Document risk acceptance (requires approval)

5.3 Emergency Patching

POL-VULN-001-10: Emergency patching for critical vulnerabilities.

Triggers:

- Active exploitation in the wild
- CVSS 9.0+ with network-exploitable
- Regulatory mandate
- CISO declaration

Process:

- Expedited change management
- Risk-based testing (abbreviated)
- Rollback plan ready
- Enhanced monitoring post-deployment

5.4 Remediation Verification

POL-VULN-001-11: Remediation shall be verified.

Requirements:

- Re-scan after remediation
- Manual verification for critical items
- Documentation of remediation
- Closure in tracking system

6. Patch Management

6.1 Patch Assessment

POL-VULN-001-12: Patches shall be assessed.

Assessment Criteria:

- Security relevance
- System compatibility
- Dependencies
- Vendor recommendations
- Known issues

6.2 Patch Testing

POL-VULN-001-13: Patches shall be tested.

Patch Priority	Testing Requirements
Critical	Abbreviated testing (4-24 hours)
High	Standard testing (48 hours)
Medium/Low	Full testing cycle

Testing Environment:

- Representative test systems
- Key application validation
- Rollback verification

6.3 Patch Deployment

POL-VULN-001-14: Patch deployment process.

Requirements:

- Change management compliance

- Deployment schedule by asset tier
- Maintenance window adherence
- Success criteria defined
- Rollback capability

6.4 Patch Compliance

POL-VULN-001-15: Patch compliance targets.

Patch Severity	Compliance Target	Measurement
Critical	95% within SLA	Weekly
High	90% within SLA	Monthly
Medium/Low	85% within SLA	Monthly

7. Application Security

7.1 Secure Development

POL-VULN-001-16: Security in development lifecycle.

Requirements:

- Security requirements in design
- Secure coding training
- SAST in CI/CD pipeline
- Code review for security
- Security testing before release

7.2 Application Scanning

POL-VULN-001-17: Application vulnerability scanning.

Scan Type	When	Scope
SAST	Every commit/build	Code changes
SCA	Every build	Dependencies
DAST	Weekly + Pre-release	Running application
IAST	During testing	Runtime analysis
Penetration Test	Annually	Full application

7.3 Third-Party Dependencies

POL-VULN-001-18: Third-party component security.

Requirements:

- Software Composition Analysis (SCA)
- Known vulnerability database checking
- License compliance verification
- Update monitoring for components

- Remediation for vulnerable components

8. Penetration Testing

8.1 Penetration Testing Program

POL-VULN-001-19: Regular penetration testing.

Test Type	Frequency	Scope
External Network	Annually	All external IPs
Internal Network	Annually	Internal infrastructure
Web Application	Annually + Major changes	All web apps
Social Engineering	Annually	Employees
Physical	Every 2 years	Facilities
Red Team	Every 2 years	Full scope

8.2 Penetration Test Management

POL-VULN-001-20: Penetration test requirements.

Requirements:

- Qualified testers (certifications: OSCP, GPEN, etc.)
- Defined rules of engagement
- Management authorization
- Findings confidentiality
- Remediation tracking

9. Exception Management

9.1 Vulnerability Exceptions

POL-VULN-001-21: Exception process for vulnerabilities.

Exception Types:

- Temporary Exception: Time-limited due to project constraints
- Risk Acceptance: Permanent acceptance with compensating controls
- False Positive: Confirmed not a real vulnerability

9.2 Exception Requirements

POL-VULN-001-22: Exception documentation requirements.

Required Information:

- Business justification
- Risk assessment
- Compensating controls
- Expiration date (for temporary)
- Approval authority

- Review schedule

Approval Authority:

Risk Level	Approver
Critical	CISO + CIO
High	CISO
Medium	Security Manager
Low	Team Lead

10. Reporting and Metrics

10.1 Vulnerability Metrics

POL-VULN-001-23: Key vulnerability metrics.

Metrics to Track:

- Total open vulnerabilities by severity
- Mean time to remediate (MTTR) by severity
- Vulnerability aging report
- Scan coverage percentage
- Patch compliance rates
- Exception count and status
- Trend analysis

10.2 Reporting Requirements

POL-VULN-001-24: Vulnerability reporting.

Report	Frequency	Audience
Operational Dashboard	Real-time	Security Team
Weekly Summary	Weekly	IT Leadership
Monthly Report	Monthly	Management
Executive Summary	Quarterly	Executive/Board

11. Tools and Technology

11.1 Vulnerability Management Platform

POL-VULN-001-25: Platform requirements.

Requirements:

- Centralized vulnerability tracking
- Integration with scanning tools
- Risk scoring and prioritization
- Workflow management
- Reporting and dashboards

- API for integration

11.2 Integration Requirements

POL-VULN-001-26: Tool integrations.

Integrations:

- CMDB for asset context
- ITSM for remediation tracking
- SIEM for correlation
- CI/CD for development pipeline
- Cloud platforms for cloud assets

12. Compliance

12.1 Regulatory Requirements

This policy supports:

- NCA Essential Cybersecurity Controls (ECC-1: 2-10)
- ISO/IEC 27001:2022 - A.12.6 Technical Vulnerability Management
- PCI DSS - Requirement 6, 11
- CIS Controls - Control 7

13. Roles and Responsibilities

CISO

- Policy ownership
- Risk acceptance authority
- Executive reporting

Security Team

- Vulnerability scanning
- Risk assessment
- Remediation coordination
- Reporting

IT Operations

- Patch deployment
- System remediation
- Change management
- Testing

System Owners

- Remediation prioritization
- Exception requests

- Compliance accountability

Development Teams

- Secure coding
- SAST/SCA remediation
- Application patching

14. Enforcement

Non-compliance may result in:

- System isolation
- Access restrictions
- Escalation to management
- Disciplinary action

15. Review

Annual review for:

- Emerging threats
- New technologies
- Process improvements
- Regulatory changes

16. References

- NCA Essential Cybersecurity Controls
- NIST SP 800-40 (Patch and Vulnerability Management)
- OWASP Vulnerability Management Guide
- CIS Controls

Document Control:

Version	Date	Author	Changes
1.0	January 2026	CISO	Initial Release