

Configuration and Hardening Policy

Organization: AegisCISO

Document ID: POL-HARD-001

Version: 1.0

Effective Date: January 2026

Classification: Internal

Owner: Chief Information Security Officer (CISO)

1. Purpose

This policy establishes requirements for secure configuration and hardening of AegisCISO information systems to reduce the attack surface and protect against security threats.

2. Scope

This policy applies to:

- All servers (physical and virtual)
- All workstations and endpoints
- All network devices (routers, switches, firewalls)
- All operating systems
- All applications and middleware
- All cloud infrastructure
- All containers and orchestration platforms

3. General Hardening Requirements

3.1 Baseline Configuration

POL-HARD-001-01: All systems shall be configured according to approved security baselines.

Requirements:

- CIS Benchmarks as primary baseline
- Vendor-specific hardening guides as secondary reference
- Deviations documented and approved
- Baselines reviewed and updated annually

3.2 Default Configuration Changes

POL-HARD-001-02: Default configurations shall be modified.

Requirements:

- Default passwords changed before deployment
- Default accounts disabled or renamed
- Default services evaluated and unnecessary ones disabled
- Default ports changed where applicable

- Sample/test data removed

3.3 Principle of Least Functionality

POL-HARD-001-03: Systems shall implement minimum required functionality.

Requirements:

- Only necessary services enabled
- Only required ports open
- Only needed software installed
- Only essential features activated
- Unused components removed

4. Operating System Hardening

4.1 Windows Server Hardening

POL-HARD-001-04: Windows servers shall be hardened.

Requirements:

- Server Core installation preferred
- Windows Firewall enabled
- Windows Defender or approved AV enabled
- BitLocker encryption enabled
- Secure boot enabled
- Credential Guard enabled
- Attack Surface Reduction rules configured

Group Policy Requirements:

- Password complexity enforced
- Account lockout configured
- Audit policy configured
- USB storage restricted
- Autorun disabled
- Remote Desktop secured (NLA required)

4.2 Linux Server Hardening

POL-HARD-001-05: Linux servers shall be hardened.

Requirements:

- Minimal installation profile
- SELinux/AppArmor enforcing mode
- Firewall (iptables/nftables/firewalld) enabled
- SSH hardening applied
- Root login disabled
- Automatic security updates enabled
- File system permissions verified

SSH Hardening Requirements:

Protocol 2

```
PermitRootLogin no
PasswordAuthentication no
PubkeyAuthentication yes
MaxAuthTries 3
AllowUsers <approved_users>
ClientAliveInterval 300
ClientAliveCountMax 2
```

4.3 Workstation Hardening

POL-HARD-001-06: Workstations shall be hardened.

Requirements:

- Full disk encryption enabled
- Local firewall enabled
- Antivirus/EDR deployed
- Application whitelisting where feasible
- USB device control implemented
- Browser hardening applied
- Auto-lock configured (5 minutes)
- BIOS/UEFI password set

5. Network Device Hardening

5.1 Router and Switch Hardening

POL-HARD-001-07: Network devices shall be hardened.

Requirements:

- Management interfaces on separate VLAN
- SNMP v3 with authentication and encryption
- SSH for management (Telnet disabled)
- Logging to central SIEM
- NTP synchronization configured
- Banner warnings displayed
- Unused ports administratively down

5.2 Firewall Hardening

POL-HARD-001-08: Firewalls shall be hardened.

Requirements:

- Default deny policy (inbound)
- Explicit allow rules only
- Rule documentation required

- Regular rule review (quarterly)
- Logging of denied traffic
- High availability configured
- Management interface isolation

5.3 Wireless Infrastructure

POL-HARD-001-09: Wireless infrastructure shall be hardened.

Requirements:

- WPA3 preferred, WPA2-Enterprise minimum
- SSID segregation (corporate, guest)
- Rogue AP detection enabled
- Client isolation on guest networks
- Strong pre-shared keys (if PSK used)
- Regular key rotation

6. Application Hardening

6.1 Web Server Hardening

POL-HARD-001-10: Web servers shall be hardened.

Requirements:

- HTTPS enforced (HTTP redirect)
- TLS 1.3/1.2 only
- Security headers implemented
- Directory listing disabled
- Server signature suppressed
- Default pages removed
- Access logging enabled

Required Security Headers:

X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
Content-Security-Policy: <appropriate policy>
Referrer-Policy: strict-origin-when-cross-origin

Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

6.2 Database Hardening

POL-HARD-001-11: Databases shall be hardened.

Requirements:

- Default accounts removed or secured
- Listener on non-default port
- Network encryption enabled

- Audit logging enabled
- Stored procedures reviewed
- Transparent Data Encryption enabled
- Backup encryption enabled

6.3 Email Server Hardening

POL-HARD-001-12: Email servers shall be hardened.

Requirements:

- TLS encryption enforced
- SPF, DKIM, DMARC configured
- Open relay prevention
- Rate limiting implemented
- Attachment filtering enabled
- Anti-malware scanning enabled

7. Cloud and Virtualization Hardening

7.1 Hypervisor Hardening

POL-HARD-001-13: Hypervisors shall be hardened.

Requirements:

- Management interface isolated
- Virtual switch security enabled
- VM encryption enabled
- Snapshot management controlled
- Resource allocation limits set
- Audit logging enabled

7.2 Cloud Infrastructure

POL-HARD-001-14: Cloud resources shall be hardened.

Requirements:

- Security groups configured (default deny)
- Encryption at rest enabled
- IAM policies follow least privilege
- Logging to central repository
- Public access restricted
- Network segmentation implemented

7.3 Container Hardening

POL-HARD-001-15: Containers shall be hardened.

Requirements:

- Minimal base images

- Non-root user in containers
- Read-only file systems where possible
- Resource limits configured
- Network policies implemented
- Image scanning in CI/CD
- Signed images only

Container Security Requirements:

```
runAsNonRoot: true
readOnlyRootFilesystem: true
allowPrivilegeEscalation: false
capabilities:
  drop:
    - ALL
```

securityCon

8. Endpoint Hardening

8.1 Mobile Device Hardening

POL-HARD-001-16: Mobile devices shall be hardened.

Requirements:

- MDM enrollment required
- Screen lock enabled (PIN/biometric)
- Encryption enabled
- Remote wipe capability
- App installation restrictions
- Jailbreak/root detection
- VPN for corporate access

8.2 IoT Device Hardening

POL-HARD-001-17: IoT devices shall be hardened.

Requirements:

- Network segmentation (separate VLAN)
- Default credentials changed
- Firmware updates applied
- Unnecessary features disabled
- Monitoring implemented
- Vendor support verified

9. Configuration Management

9.1 Configuration Documentation

POL-HARD-001-18: Configurations shall be documented.

Requirements:

- Baseline configurations documented
- Configuration changes logged
- Change approvals documented
- Configuration repository maintained
- Version control implemented

9.2 Configuration Monitoring

POL-HARD-001-19: Configuration compliance shall be monitored.

Requirements:

- Automated configuration scanning
- Deviation alerting
- Compliance dashboards
- Regular compliance reports
- Remediation tracking

9.3 Configuration Change Control

POL-HARD-001-20: Configuration changes shall be controlled.

Requirements:

- Change request required
- Security review for changes
- Testing before deployment
- Rollback plan documented
- Post-change verification

10. Patch Management

10.1 Patch Assessment

POL-HARD-001-21: Security patches shall be assessed and applied.

Patch Timelines:

Severity	Assessment	Deployment
Critical	24 hours	72 hours
High	72 hours	7 days
Medium	7 days	30 days
Low	30 days	90 days

10.2 Patch Testing

POL-HARD-001-22: Patches shall be tested before deployment.

Requirements:

- Test environment validation
- Application compatibility testing
- Rollback procedure verified
- Deployment plan documented

11. Compliance Verification

11.1 Hardening Assessment

POL-HARD-001-23: Hardening compliance shall be verified.

Requirements:

- Quarterly automated scanning
- Annual manual assessment
- Vulnerability scanning integration
- Compliance reporting

11.2 Audit Trail

POL-HARD-001-24: Configuration audit trail shall be maintained.

Requirements:

- All changes logged
- Before/after states captured
- Change approver recorded
- Retention for 3 years minimum

12. Exceptions

12.1 Exception Process

Hardening exceptions require:

- Business justification
- Risk assessment
- Compensating controls
- Time-limited approval
- Regular review
- CISO approval

13. Roles and Responsibilities

CISO

- Policy ownership
- Exception approval
- Compliance oversight

Security Team

- Baseline definition
- Compliance monitoring
- Security assessments

IT Operations

- Configuration implementation
- Patch deployment
- Compliance remediation

System Owners

- System-specific hardening
- Change management
- Compliance reporting

14. Enforcement

Non-compliance may result in:

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

15. Review

This policy shall be reviewed annually and updated for:

- New system types
- Emerging threats
- Vendor guidance updates
- Regulatory changes

16. References

- NCA Configuration and Hardening Policy Template
- CIS Benchmarks
- DISA STIGs
- NIST SP 800-123 (Server Security)
- NIST SP 800-70 (Security Configuration Checklists)

Document Control:

Version	Date	Author	Changes
1.0	January 2026	CISO	Initial Release