Network Security Policy

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

---

1. Purpose

This policy establishes requirements for securing AegisCISO network infrastructure to protect information assets from unauthorized access, threats, and ensure availability of network services.

2. Scope

This policy applies to:

- All network infrastructure (routers, switches, firewalls, load balancers)
- All network connections (wired, wireless, remote)
- All network services and protocols
- All personnel managing or using network resources

3. Network Architecture

3.1 Network Segmentation

POL-NET-001-01: Networks shall be segmented based on security requirements.

Required Segments:

Segment	Purpose	Security Level
DMZ	Public-facing services	High
Production	Business applications	Critical
Development	Development/testing	Medium
Corporate	End-user workstations	Medium
Management	Network/security management	Critical
Guest	Visitor network access	Low
IoT	Internet of Things devices	Medium

3.2 Network Zones

POL-NET-001-02: Security zones shall be defined and controlled.

Zone Requirements:

- Clear boundary definition
- Traffic flow documentation
- Inter-zone traffic controlled by firewall

- Default deny between zones
- Logging of cross-zone traffic

3.3 VLAN Configuration

POL-NET-001-03: VLANs shall be used for logical segmentation.

Requirements:

- Separate VLANs for different security requirements
- VLAN hopping prevention enabled
- Native VLAN changed from default
- Unused ports in dedicated VLAN
- Management traffic on dedicated VLAN

4. Perimeter Security

4.1 Firewall Requirements

POL-NET-001-04: Firewalls shall protect all network boundaries.

Requirements:

- Next-generation firewalls at internet boundary
- Internal firewalls between security zones
- Default deny policy (inbound and outbound)
- Stateful inspection enabled
- Application-aware filtering
- High availability configuration

4.2 Firewall Rule Management

POL-NET-001-05: Firewall rules shall be managed.

Requirements:

- All rules documented with business justification
- Rule owner identified
- Temporary rules with expiration dates
- Quarterly rule review
- Unused rules removed
- Change control for rule modifications

4.3 Intrusion Detection/Prevention

POL-NET-001-06: IDS/IPS shall be deployed.

Requirements:

- IDS/IPS at network perimeter
- Internal IDS for critical segments
- Signature updates automated
- Custom rules for environment

- Alerts integrated with SIEM
- Regular tuning to reduce false positives

4.4 Web Application Firewall

POL-NET-001-07: WAF shall protect web applications.

Requirements:

- WAF for all internet-facing web applications
- OWASP ruleset enabled
- Custom rules as needed
- SSL/TLS termination
- Bot management enabled
- Regular rule updates

5. Internal Network Security

5.1 Switch Security

POL-NET-001-08: Switches shall be secured.

Requirements:

- Port security enabled (MAC limiting)
- DHCP snooping enabled
- Dynamic ARP inspection enabled
- Storm control configured
- Spanning tree protection enabled
- Unused ports disabled

5.2 Router Security

POL-NET-001-09: Routers shall be secured.

Requirements:

- Access control lists configured
- Routing protocol authentication
- ICMP rate limiting
- Source routing disabled
- IP spoofing prevention (uRPF)
- Logging enabled

5.3 Network Access Control

POL-NET-001-10: NAC shall control network access.

Requirements:

- 802.1X authentication for wired connections
- Device posture assessment
- Guest network isolation

- Remediation VLAN for non-compliant devices
- MAC authentication bypass for approved devices

6. Remote Access

6.1 VPN Requirements

POL-NET-001-11: VPN shall be used for remote access.

Requirements:

- IPsec or SSL VPN only
- Strong authentication (MFA required)
- Split tunneling disabled
- Session timeout configured
- Encryption: AES-256
- Perfect Forward Secrecy enabled

6.2 Site-to-Site VPN

POL-NET-001-12: Site-to-site connectivity requirements.

Requirements:

- IPsec with IKEv2
- Pre-shared keys rotated annually (certificates preferred)
- Traffic encryption: AES-256-GCM
- Dead peer detection enabled
- Redundant tunnels where critical

6.3 Third-Party Remote Access

POL-NET-001-13: Third-party remote access controls.

Requirements:

- Dedicated VPN profiles
- Time-limited access
- Jump server/bastion host required
- Session recording enabled
- Access logging and monitoring

7. Wireless Security

7.1 Corporate Wireless

POL-NET-001-14: Corporate wireless requirements.

Requirements:

- WPA3-Enterprise (WPA2-Enterprise minimum)
- 802.1X authentication (EAP-TLS preferred)

- SSID not broadcast (optional)
- Management frames protection
- Regular key rotation
- Rogue AP detection

7.2 Guest Wireless

POL-NET-001-15: Guest wireless requirements.

Requirements:

- Separate SSID and network
- Internet-only access
- Client isolation enabled
- Captive portal with terms of use
- Bandwidth throttling
- Time-limited access

7.3 Wireless Monitoring

POL-NET-001-16: Wireless monitoring requirements.

Requirements:

- Rogue AP detection and alerting
- Wireless IDS enabled
- Signal coverage analysis
- Regular wireless security assessments

8. DNS and DHCP Security

8.1 DNS Security

POL-NET-001-17: DNS security requirements.

Requirements:

- Internal DNS servers only
- DNSSEC where supported
- DNS logging enabled
- DNS query filtering
- Split-horizon DNS
- DNS over HTTPS/TLS for sensitive traffic

8.2 DHCP Security

POL-NET-001-18: DHCP security requirements.

Requirements:

- Authorized DHCP servers only
- DHCP snooping on switches
- IP address management documented

- Lease time appropriate to environment
- Logging of DHCP transactions

9. Network Monitoring

9.1 Traffic Monitoring

POL-NET-001-19: Network traffic shall be monitored.

Requirements:

- NetFlow/sFlow collection from key points
- Full packet capture capability
- Baseline traffic patterns established
- Anomaly detection enabled
- Alert thresholds configured

9.2 Logging Requirements

POL-NET-001-20: Network device logging.

Minimum Events to Log:

- Configuration changes
- Authentication events
- Administrative access
- ACL/firewall denies
- Routing changes
- Interface state changes

Log Requirements:

- Central log collection (SIEM)
- Log integrity protection
- Retention minimum 1 year
- Time synchronization (NTP)

10. Network Device Management

10.1 Management Access

POL-NET-001-21: Network device management requirements.

Requirements:

- Management interface on dedicated VLAN
- SSH only (Telnet disabled)
- HTTPS for web management
- SNMP v3 with authentication
- Management ACLs configured
- MFA for administrative access

10.2 Configuration Management

POL-NET-001-22: Network configuration management.

Requirements:

- Configuration backup automated
- Version control for configurations
- Change management process followed
- Configuration templates standardized
- Regular configuration review

10.3 Firmware/Software Management

POL-NET-001-23: Network device updates.

Requirements:

- Regular firmware updates
- Security patches prioritized
- Testing before production deployment
- Rollback procedures documented
- EOL device replacement plan

11. Cloud Network Security

11.1 Cloud Connectivity

POL-NET-001-24: Cloud network security requirements.

Requirements:

- Direct connect or VPN for cloud access
- Cloud security groups configured (default deny)
- Network ACLs layered with security groups
- VPC peering controlled and documented
- Transit gateway for multi-VPC architecture

11.2 Hybrid Network

POL-NET-001-25: Hybrid network requirements.

Requirements:

- Consistent security policy across environments
- Identity-aware access for cloud resources
- Traffic encryption between on-premises and cloud
- Monitoring across hybrid environment

12. Protocol Security

12.1 Approved Protocols

POL-NET-001-26: Network protocol requirements.

Category	Approved	Prohibited
Remote Access	SSH v2, RDP (with NLA)	Telnet, rlogin
File Transfer	SFTP, SCP, HTTPS	FTP, TFTP
Email	SMTP with TLS, IMAPS	Unencrypted SMTP/IMAP
Web	HTTPS	HTTP (except redirect)
Management	HTTPS, SSH, SNMPv3	HTTP, SNMPv1/v2
Routing	With authentication	Without authentication

12.2 Protocol Inspection

POL-NET-001-27: Protocol inspection requirements.

Requirements:

- SSL/TLS inspection for outbound traffic (with exceptions)
- Protocol enforcement on firewalls
- Protocol anomaly detection

13. Compliance

13.1 Regulatory Requirements

This policy supports:

- NCA Essential Cybersecurity Controls (ECC-1: 2-8)
- ISO/IEC 27001:2022 - A.13 Communications Security
- PCI DSS - Requirement 1
- CIS Controls

14. Roles and Responsibilities

Network Team

- Implement network security controls
- Maintain network documentation
- Monitor network security
- Respond to network incidents

Security Team

- Define network security requirements
- Review network architecture
- Conduct security assessments
- Monitor for threats

CISO

- Policy ownership

- Exception approval
- Compliance oversight

15. Enforcement

Non-compliance may result in:

- Network access revocation
- System isolation
- Disciplinary action
- Security investigation

16. Review

Annual review for:

- Technology changes
- New threats
- Regulatory updates
- Incident lessons learned

17. References

- NCA Essential Cybersecurity Controls
- CIS Benchmarks (Network Devices)
- NIST SP 800-41 (Firewall Guidelines)
- NIST SP 800-77 (IPsec VPNs)

Document Control:

Version	Date	Author	Changes
1.0	January 2026	CISO	Initial Release