Corporate Cybersecurity Policy

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

1. Purpose

This policy establishes the corporate cybersecurity framework for AegisCISO to protect information assets, ensure business continuity, and maintain compliance with applicable laws and regulations including NCA Essential Cybersecurity Controls (ECC).

2. Scope

This policy applies to:

- All employees, contractors, and third parties with access to AegisCISO information systems
- All information assets including data, hardware, software, and network resources
- All locations and facilities operated by AegisCISO
- All cloud services and third-party systems processing AegisCISO data

3. Policy Statements

3.1 Cybersecurity Governance

- A Cybersecurity Department shall be established with direct reporting to executive management
- The CISO shall have the authority and resources necessary to implement this policy
- Cybersecurity roles and responsibilities shall be clearly defined and documented
- Regular reporting to the Board of Directors on cybersecurity posture shall be conducted

3.2 Risk Management

- A formal cybersecurity risk management process shall be implemented
- Risk assessments shall be conducted annually and upon significant changes
- Risk treatment plans shall be developed and tracked to completion
- Risk appetite and tolerance levels shall be defined by executive management

3.3 Asset Management

- All information assets shall be inventoried and classified
- Asset owners shall be assigned for all critical assets
- Asset lifecycle management processes shall be implemented
- Unauthorized assets shall be prohibited on the corporate network

3.4 Human Resources Security

- Background verification shall be conducted for all employees and contractors
- Cybersecurity awareness training shall be mandatory for all personnel
- Acceptable use policies shall be acknowledged by all users
- Termination procedures shall include immediate access revocation

3.5 Physical Security

- Physical access controls shall protect all facilities housing information systems
- Visitor access shall be logged and escorted in sensitive areas
- Environmental controls shall protect against natural and man-made threats
- Equipment disposal shall follow secure sanitization procedures

3.6 Access Control

- Access shall be granted based on the principle of least privilege
- Strong authentication mechanisms shall be implemented
- Privileged access shall be restricted and monitored
- Access reviews shall be conducted quarterly

3.7 Cryptography

- Approved cryptographic algorithms shall be used for data protection
- Encryption shall be implemented for data at rest and in transit
- Key management procedures shall be documented and followed
- Certificate lifecycle management shall be implemented

3.8 Operations Security

- Change management procedures shall be followed for all systems
- Capacity management shall ensure adequate resources
- Malware protection shall be deployed on all endpoints
- Logging and monitoring shall be implemented across all systems

3.9 Communications Security

- Network segmentation shall separate critical systems
- Firewalls and intrusion detection systems shall be deployed
- Secure protocols shall be used for all communications
- Email and web filtering shall be implemented

3.10 System Development Security

- Secure development lifecycle practices shall be followed
- Security testing shall be conducted before production deployment
- Third-party code shall be reviewed for security vulnerabilities
- Production data shall not be used in development environments

3.11 Supplier Security

- Third-party security assessments shall be conducted before engagement

- Security requirements shall be included in all contracts
- Supplier compliance shall be monitored throughout the relationship
- Right to audit clauses shall be included in contracts

3.12 Incident Management

- A cybersecurity incident response plan shall be maintained
- Incidents shall be reported within 24 hours of detection
- Post-incident reviews shall be conducted and lessons learned documented
- Incident response capabilities shall be tested annually

3.13 Business Continuity

- Business impact analysis shall identify critical systems
- Disaster recovery plans shall be documented and tested
- Backup procedures shall ensure data availability
- Recovery time objectives shall be defined and achievable

3.14 Compliance

- Applicable laws, regulations, and contractual requirements shall be identified
- Compliance assessments shall be conducted annually
- Audit findings shall be tracked to remediation
- Privacy requirements shall be implemented and maintained

4. Sub-Policies

This Corporate Cybersecurity Policy is supported by the following sub-policies:

1. Access Control Policy
2. Acceptable Use Policy
3. Asset Management Policy
4. Backup and Recovery Policy
5. Business Continuity Policy
6. Change Management Policy
7. Cloud Security Policy
8. Configuration and Hardening Policy
9. Cryptography Policy
10. Data Classification Policy
11. Data Protection Policy
12. Email Security Policy
13. Endpoint Security Policy
14. Human Resources Cybersecurity Policy
15. Incident Response Policy
16. Information Security Policy
17. Logging and Monitoring Policy
18. Mobile Device Policy

19. Network Security Policy
20. Password Policy
21. Patch Management Policy
22. Physical Security Policy
23. Privacy Policy
24. Remote Access Policy
25. Risk Management Policy
26. Secure Development Policy
27. Security Awareness Policy
28. Third-Party Security Policy
29. Vulnerability Management Policy
30. Wireless Security Policy

5. Roles and Responsibilities

Board of Directors

- Approve the cybersecurity strategy and budget
- Receive regular reports on cybersecurity posture
- Ensure adequate resources for cybersecurity program

Executive Management

- Ensure policy implementation and compliance
- Allocate resources for cybersecurity initiatives
- Foster a security-aware culture

Chief Information Security Officer (CISO)

- Develop and maintain cybersecurity policies
- Lead the cybersecurity program
- Report on security metrics and incidents
- Ensure regulatory compliance

Department Managers

- Implement security controls within their areas
- Ensure staff compliance with policies
- Report security incidents promptly

All Employees

- Comply with all cybersecurity policies
- Complete required security training
- Report suspected security incidents
- Protect information assets

6. Enforcement

Violations of this policy may result in disciplinary action up to and including termination of employment. Contractors and third parties may have their access revoked and contracts terminated. Legal action may be taken where appropriate.

7. Review and Updates

This policy shall be reviewed annually and updated as needed to address:

- Changes in business operations
- New or emerging threats
- Regulatory changes
- Lessons learned from incidents

8. References

- NCA Essential Cybersecurity Controls (ECC)
- NCA Cybersecurity Toolkit
- ISO/IEC 27001:2022
- NIST Cybersecurity Framework

Document Control:

Version	Date	Author	Changes
1.0	January 2026	CISO	Initial Release