Cryptography Policy

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

1. Purpose

This policy establishes the requirements for cryptographic controls to protect the confidentiality, integrity, and authenticity of AegisCISO information assets in accordance with regulatory requirements and industry best practices.

2. Scope

This policy applies to:

- All cryptographic implementations within AegisCISO systems
- All data encryption at rest and in transit
- All digital certificates and key management
- All personnel responsible for cryptographic systems
- All third-party systems processing AegisCISO encrypted data

3. Approved Cryptographic Standards

3.1 Symmetric Encryption Algorithms

POL-CRYPT-001-01: Only approved symmetric encryption algorithms shall be used.

Algorithm	Key Length	Use Case	Status
AES	256-bit	Data at rest, file encryption	Approved
AES	128-bit	Data in transit (TLS)	Approved
ChaCha20-Poly1305	256-bit	Mobile/embedded systems	Approved
3DES	168-bit	Legacy systems only	Deprecated
DES	56-bit	Any	Prohibited

3.2 Asymmetric Encryption Algorithms

POL-CRYPT-001-02: Only approved asymmetric encryption algorithms shall be used.

Algorithm	Key Length	Use Case	Status
RSA	4096-bit	Digital signatures, key exchange	Approved
RSA	2048-bit	Short-term certificates only	Approved (until 2028)
RSA	<2048-bit	Any	Prohibited

ECDSA	P-384 (secp384r1)	Digital signatures	Approved
ECDSA	P-256 (secp256r1)	Digital signatures	Approved
Ed25519	255-bit	Digital signatures	Approved
X25519	255-bit	Key exchange	Approved

3.3 Hash Functions

POL-CRYPT-001-03: Only approved hash functions shall be used.

Algorithm	Output Size	Use Case	Status
SHA-384	384-bit	Digital signatures, high security	Approved
SHA-256	256-bit	General purpose hashing	Approved
SHA-512	512-bit	Password hashing (with salt)	Approved
SHA-1	160-bit	Legacy verification only	Deprecated
MD5	128-bit	Any security purpose	Prohibited

3.4 Key Derivation Functions

POL-CRYPT-001-04: Approved key derivation functions shall be used for password storage.

Algorithm	Parameters	Use Case	Status
Argon2id	Memory: 64MB, Iterations: 3	Password hashing	Approved
bcrypt	Cost factor: 12+	Password hashing	Approved
PBKDF2-SHA256	100,000+ iterations	Key derivation	Approved
scrypt	N=2^14, r=8, p=1	Password hashing	Approved

4. Data Encryption Requirements

4.1 Data at Rest

POL-CRYPT-001-05: Sensitive data shall be encrypted at rest.

Requirements:

- Full disk encryption on all laptops and mobile devices
- Database encryption for sensitive data columns
- File-level encryption for sensitive documents
- Backup encryption mandatory
- Encryption keys stored separately from encrypted data

Data Classification Encryption Requirements:

Classification	Encryption Required	Algorithm
Public	Optional	AES-128 minimum
Internal	Required	AES-256
Confidential	Required	AES-256
Restricted	Required	AES-256 + additional controls

4.2 Data in Transit

POL-CRYPT-001-06: Data in transit shall be encrypted using approved protocols.

Requirements:

- TLS 1.3 preferred, TLS 1.2 minimum
- SSL and TLS 1.0/1.1 prohibited
- Perfect Forward Secrecy (PFS) required
- Certificate validation mandatory
- HSTS implementation required for web applications

Approved TLS Cipher Suites:

```
TLS_AES_256_
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
```

4.3 Database Encryption

POL-CRYPT-001-07: Database encryption requirements.

Requirements:

- Transparent Data Encryption (TDE) for database files
- Column-level encryption for highly sensitive fields
- Encrypted database connections mandatory
- Encryption key rotation annually

5. Key Management

5.1 Key Generation

POL-CRYPT-001-08: Cryptographic keys shall be generated securely.

Requirements:

- Keys generated using approved random number generators
- Hardware Security Modules (HSM) for high-value keys
- Key generation in secure environment
- Dual control for master keys
- Documentation of key generation procedures

5.2 Key Storage

POL-CRYPT-001-09: Cryptographic keys shall be protected in storage.

Requirements:

- Hardware Security Modules (HSM) for production keys
- Key encryption keys (KEK) for software-stored keys
- Separation of keys from encrypted data

- Access control for key storage systems
- No keys in source code or configuration files

Key Storage Requirements by Type:

Key Type	Storage Method	Access Control
Root/Master Keys	HSM	Dual control, M of N
Production Keys	HSM or encrypted vault	Role-based, logged
Development Keys	Encrypted vault	Developer access
User Keys	Encrypted user storage	User only

5.3 Key Distribution

POL-CRYPT-001-10: Keys shall be distributed securely.

Requirements:

- Encrypted channels for key distribution
- Out-of-band verification for critical keys
- Key agreement protocols where applicable
- Documentation of key recipients
- No keys transmitted via email or chat

5.4 Key Rotation

POL-CRYPT-001-11: Cryptographic keys shall be rotated periodically.

Key Rotation Schedule:

Key Type	Rotation Frequency	Maximum Lifetime
TLS Certificates	1 year	398 days
Encryption Keys (data at rest)	2 years	3 years
Signing Keys	2 years	5 years
User Authentication Keys	1 year	2 years
Session Keys	Per session	24 hours
API Keys	1 year	2 years

5.5 Key Backup and Recovery

POL-CRYPT-001-12: Key backup and recovery procedures shall be established.

Requirements:

- Secure backup of all critical keys
- Geographic separation of key backups
- Regular recovery testing
- Dual control for key recovery
- Documentation of recovery procedures

5.6 Key Destruction

POL-CRYPT-001-13: Keys shall be securely destroyed when no longer needed.

Requirements:

- Cryptographic erasure for key destruction
- Documentation of key destruction
- Multiple witness for critical keys
- Verification of destruction
- Retention of destruction records

6. Certificate Management

6.1 Certificate Authority

POL-CRYPT-001-14: Certificates shall be obtained from approved sources.

Approved Certificate Sources:

- Internal Enterprise PKI (for internal systems)
- Commercial CAs on approved list (for external systems)
- Self-signed certificates prohibited for production

6.2 Certificate Lifecycle

POL-CRYPT-001-15: Certificate lifecycle shall be managed.

Requirements:

- Certificate inventory maintained
- Expiration monitoring (90, 60, 30 days alerts)
- Renewal process documented
- Revocation procedures established
- Certificate transparency logging

6.3 Certificate Requirements

POL-CRYPT-001-16: Minimum certificate requirements.

Requirements:

- RSA 2048-bit minimum (4096-bit preferred)
- ECDSA P-256 or P-384
- SHA-256 or stronger signature
- Subject Alternative Names (SAN) for all domains
- Extended Validation (EV) for customer-facing systems

7. Public Key Infrastructure (PKI)

7.1 PKI Architecture

POL-CRYPT-001-17: Enterprise PKI shall be maintained.

Requirements:

- Offline Root CA
- Online Issuing CAs
- Hardware protection for CA keys
- Certificate Policy (CP) documented
- Certification Practice Statement (CPS) maintained

7.2 PKI Operations

POL-CRYPT-001-18: PKI operational requirements.

Requirements:

- Separation of duties for PKI administration
- Audit logging of all PKI operations
- Regular PKI security assessments
- Disaster recovery for PKI systems
- Compliance with industry standards

8. Application Cryptography

8.1 Development Requirements

POL-CRYPT-001-19: Secure cryptographic implementation in applications.

Requirements:

- Use approved cryptographic libraries only
- No custom cryptographic implementations
- Secure random number generation
- Input validation for cryptographic functions
- Secure memory handling for keys

Approved Cryptographic Libraries:

- OpenSSL 3.x
- BoringSSL
- libsodium
- Bouncy Castle
- Windows CryptoAPI NG

8.2 Code Review

POL-CRYPT-001-20: Cryptographic implementations shall be reviewed.

Requirements:

- Security review of cryptographic code
- Static analysis for cryptographic issues
- Penetration testing of cryptographic systems
- Third-party audit for critical systems

9. Compliance and Audit

9.1 Compliance Requirements

This policy aligns with:

- NCA Essential Cybersecurity Controls (ECC-1: 2-9)
- ISO/IEC 27001:2022 - A.10 Cryptographic Controls
- PCI DSS - Requirement 3, 4
- GDPR - Article 32

9.2 Audit and Monitoring

Requirements:

- Annual cryptographic controls assessment
- Key management audit
- Certificate inventory audit
- Compliance verification

10. Exceptions

10.1 Exception Process

Exceptions to this policy require:

- Business justification
- Risk assessment
- Compensating controls
- CISO approval
- Time-limited exception (maximum 1 year)
- Regular review

11. Roles and Responsibilities

CISO

- Policy ownership and updates
- Exception approval
- Compliance oversight

Security Team

- Cryptographic standards definition
- Key management oversight
- Security assessments

IT Operations

- PKI management
- Certificate deployment
- Key backup and recovery

Development Teams

- Secure cryptographic implementation
- Use of approved libraries
- Code security review

12. Enforcement

Violations of this policy may result in:

- Disciplinary action
- Access revocation
- System isolation
- Legal action if applicable

13. Review

This policy shall be reviewed annually and updated for:

- New cryptographic standards
- Algorithm deprecation
- Regulatory changes
- Security incidents

14. References

- NCA Cryptography Policy Template
- NIST SP 800-57 (Key Management)
- NIST SP 800-131A (Cryptographic Standards)
- RFC 8446 (TLS 1.3)

Document Control:

Version	Date	Author	Changes
1.0	January 2026	CISO	Initial Release