Cryptography Policy Template

Document Control Information

- **Document Title:** Cryptography Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Cryptography Policy establishes [ORGANIZATION NAME]'s requirements for the use of cryptographic controls to protect the confidentiality, integrity, authenticity, and non-repudiation of information in accordance with ISO 27001:2022 requirements. It provides a framework for the proper implementation and management of cryptographic technologies.

1.2 Scope

This policy applies to: - All information systems and applications that store, process, or transmit sensitive information - All forms of encryption and cryptographic controls used within the organization - All employees, contractors, consultants, and third parties who implement or use cryptographic controls - All environments, including production, development, test, and disaster recovery

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Implementing appropriate cryptographic controls based on risk assessment - Using industry-standard cryptographic algorithms, protocols, and key lengths - Properly managing cryptographic keys throughout their lifecycle - Complying with relevant legal, regulatory, and contractual requirements - Regularly reviewing and updating cryptographic controls to address evolving threats

2. Cryptographic Requirements

2.1 Risk Assessment

- The need for cryptographic controls shall be determined based on risk assessment
- The type and strength of cryptographic controls shall be proportionate to the risk
- Risk assessments shall consider:
    - Confidentiality requirements of the information
    - Integrity requirements of the information
    - Authentication and non-repudiation requirements
    - Regulatory and compliance requirements
    - Potential impact of compromise
    - Technical environment and constraints

2.2 Approved Cryptographic Algorithms

[ORGANIZATION NAME] shall use only industry-standard, publicly reviewed cryptographic algorithms, including:

2.2.1 Symmetric Encryption

- Advanced Encryption Standard (AES) with minimum 256-bit key length
- [LIST OTHER APPROVED SYMMETRIC ALGORITHMS]

2.2.2 Asymmetric Encryption

- RSA with minimum 2048-bit key length
- Elliptic Curve Cryptography (ECC) with minimum 256-bit key length
- [LIST OTHER APPROVED ASYMMETRIC ALGORITHMS]

2.2.3 Hashing Algorithms

- Secure Hash Algorithm 2 (SHA-2) family (SHA-256, SHA-384, SHA-512)
- Secure Hash Algorithm 3 (SHA-3) family
- [LIST OTHER APPROVED HASHING ALGORITHMS]

2.2.4 Digital Signatures

- RSA with minimum 2048-bit key length and SHA-256 or stronger
- ECDSA with minimum 256-bit key length
- [LIST OTHER APPROVED DIGITAL SIGNATURE ALGORITHMS]

2.3 Prohibited Cryptographic Algorithms

The following algorithms are considered insecure and shall not be used: - Data Encryption Standard (DES) - Triple DES (3DES) - RC4 - MD5 - SHA-1 - [LIST OTHER PROHIBITED ALGORITHMS]

2.4 Cryptographic Protocols

[ORGANIZATION NAME] shall use only secure cryptographic protocols, including:

2.4.1 Secure Communications

- Transport Layer Security (TLS) version 1.2 or higher
- Secure Shell (SSH) version 2 or higher
- IPsec with strong algorithms and perfect forward secrecy
- [LIST OTHER APPROVED COMMUNICATION PROTOCOLS]

2.4.2 Prohibited Protocols

The following protocols are considered insecure and shall not be used: - Secure Sockets Layer (SSL) all versions - TLS versions 1.0 and 1.1 - SSH version 1 - [LIST OTHER PROHIBITED PROTOCOLS]

3. Key Management

3.1 Key Generation

- Cryptographic keys shall be generated using approved random number generators
- Keys shall be generated in a secure environment
- Key generation shall be performed by authorized personnel or automated systems
- Key generation events shall be logged
- Key length shall comply with industry standards and best practices

3.2 Key Distribution

- Keys shall be distributed using secure methods
- Keys shall be protected during distribution
- Out-of-band methods should be used for initial key exchange where possible
- Key distribution shall be logged
- Recipients shall acknowledge receipt of keys where appropriate

3.3 Key Storage

- Private and secret keys shall be stored securely
- Keys shall be protected against unauthorized access, modification, and disclosure
- Hardware Security Modules (HSMs) should be used for critical keys
- Keys shall never be stored in clear text
- Key storage systems shall be physically and logically secured

3.4 Key Usage

- Keys shall be used only for their intended purpose
- Different keys shall be used for different functions
- Keys shall be used in accordance with any limitations (time period, data, transactions)
- Key usage shall be logged where appropriate
- Separation of duties shall be implemented for critical key operations

3.5 Key Rotation

- Encryption keys shall be changed (rotated) at regular intervals
- Key rotation frequency shall be based on:
  - Sensitivity of the protected information
  - Volume of data protected by the key
  - Exposure of the key
  - Industry standards and best practices
- Key rotation shall be performed without service disruption where possible
- Key rotation events shall be logged

3.6 Key Backup and Recovery

- Critical keys shall be backed up to prevent loss
- Key backups shall be secured at the same level as operational keys
- Key recovery procedures shall be documented and tested
- Key recovery shall require multiple authorized individuals (M of N control)
- Key recovery events shall be logged

3.7 Key Revocation and Destruction

- Keys shall be revoked when compromised or no longer needed
- Revoked keys shall be destroyed securely
- Key destruction shall ensure keys cannot be recovered
- Key revocation and destruction shall be logged
- Key revocation information shall be distributed to all relevant parties

4. Cryptographic Implementation

4.1 Data at Rest

- Sensitive data stored in databases shall be encrypted
- Sensitive files and documents shall be encrypted
- Full disk encryption shall be used on laptops and mobile devices
- Backup media containing sensitive information shall be encrypted
- Encryption keys shall be stored separately from encrypted data

4.2 Data in Transit

- Sensitive data transmitted over networks shall be encrypted
- All external communications shall use secure protocols
- Internal network segments with sensitive data shall use encryption
- Remote access shall use encrypted channels
- Web applications shall use HTTPS with strong TLS configuration

4.3 Data in Use

- Memory protection mechanisms shall be implemented where possible
- Sensitive data shall be protected in memory
- Cryptographic operations shall be performed in secure environments
- Cryptographic keys shall be protected in memory

4.4 Authentication and Digital Signatures

- Authentication systems shall use strong cryptographic methods
- Digital signatures shall be used to verify document authenticity where required
- Digital signatures shall be used for code signing
- Non-repudiation shall be implemented for critical transactions
- Certificates shall be obtained from trusted Certificate Authorities

5. Cryptographic Systems and Services

5.1 Cryptographic Modules

- Cryptographic modules shall be validated to FIPS 140-2/3 or equivalent standards where possible
- Cryptographic modules shall be properly configured and maintained
- Cryptographic modules shall be tested before deployment
- Vulnerabilities in cryptographic modules shall be addressed promptly

5.2 Certificate Management

- Digital certificates shall be obtained from trusted Certificate Authorities
- Internal PKI systems shall be properly secured and managed
- Certificate validity periods shall align with industry standards
- Certificate revocation checking shall be implemented
- Certificate renewal processes shall be documented and followed

5.3 Random Number Generation

- Only cryptographically secure random number generators shall be used
- Random number generators shall be tested for sufficient entropy
- Hardware random number generators should be used where available
- Pseudo-random number generators shall be properly seeded

5.4 Cryptographic Services

- Cryptographic services shall be properly authenticated and authorized
- Cryptographic services shall be monitored and logged
- Cryptographic services shall be included in business continuity planning
- Cryptographic services shall be tested regularly

6. Compliance and Exceptions

6.1 Legal and Regulatory Compliance

- Cryptographic controls shall comply with relevant laws and regulations
- Export/import restrictions on cryptography shall be observed
- Key disclosure requirements shall be understood and documented
- Compliance shall be regularly reviewed and documented

6.2 Exceptions

Exceptions to this policy shall be: - Documented with justification - Risk-assessed and approved by the Information Security Manager - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate

7. Roles and Responsibilities

7.1 Information Security Manager

- Develop and maintain the Cryptography Policy
- Approve cryptographic standards and algorithms

- Review and approve exceptions to this policy
- Ensure compliance with this policy

7.2 IT Department

- Implement cryptographic controls according to this policy
- Manage cryptographic systems and services
- Monitor cryptographic systems for security issues
- Maintain documentation of cryptographic implementations

7.3 Key Custodians

- Generate and manage cryptographic keys
- Implement key management procedures
- Protect keys from unauthorized access
- Maintain key inventory and documentation

7.4 System Owners

- Identify data requiring cryptographic protection
- Ensure cryptographic controls are implemented for their systems
- Verify cryptographic controls are functioning properly
- Report cryptographic issues or incidents

7.5 All Users

- Protect encryption keys and passwords assigned to them
- Use cryptographic tools according to instructions
- Report suspected compromises of cryptographic controls
- Comply with all aspects of this policy

8. Monitoring and Review

8.1 Monitoring

- Cryptographic systems shall be monitored for proper operation
- Key usage shall be logged and reviewed
- Unauthorized access attempts shall be detected and reported
- Cryptographic performance shall be monitored

8.2 Policy Review

This policy shall be reviewed: - At least annually - When significant changes occur in the threat landscape - When new cryptographic vulnerabilities are discovered - When relevant laws or regulations change - After security incidents related to cryptography

9. Related Documents

- Information Security Policy
- Data Protection Policy
- Access Control Policy
- Key Management Procedure
- Certificate Management Procedure
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

10. Approval

This Cryptography Policy is approved by:

Name: _____ Position: _____ Date: _____ Signature: _____