# Cryptography Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives and legal requirements.*

### Security boundary under scope

1. [List of applicable systems]

### References

1. NIST 800-52: <https://csrc.nist.gov/pubs/sp/800/52/r2/final>
2. NIST FIPS 140-3: <https://csrc.nist.gov/pubs/fips/140-3/final>
3. NIST 800-175A: <https://csrc.nist.gov/pubs/sp/800/175/a/final>
4. NIST 800-175B: <https://csrc.nist.gov/pubs/sp/800/175/b/r1/final>
5. NIST FIPS 140-3: <https://csrc.nist.gov/pubs/fips/140-3/final>
6. NIST SP 800-153: <https://csrc.nist.gov/pubs/sp/800/153/final>
7. NIST 800-57: <https://csrc.nist.gov/projects/key-management/key-management-guidelines>
8. NIST 800-131: <https://csrc.nist.gov/pubs/sp/800/131/a/r2/final>
9. ISO/IEC 11770: <https://webstore.ansi.org/industry/software/encryption-cryptography/key-management>
10. ISO/IEC 27033-6: <https://www.iso.org/standard/51585.html>
11. ISO/IEC 18033: <https://www.iso.org/standard/76156.html>
12. ISO/IEC 20648: <https://www.iso.org/standard/76156.html>
13. ISO/IEC 27099: <https://www.iso.org/standard/56590.html>
14. ISO/IEC 27001:2022: A.8.20, A.8.24
15. NIST 800-53 rev. 5: AC-17(2), AC-18, AC-18(1), AC-19(5), CP-9(8), CP-5, IA-5(2), IA-7, SC-7(4), SC-8, SC-8(1), SC-12, SC-13, SC-17, SC-28, SC-28(1)
16. CIS v8: 3.9, 3.10, 3.11, 12.3, 12.6, 12.7
17. PCI DSS 4.0: 2.3.2, 3.1.1, 3.3.2, 3.3.3, 3.5.1, 3.5.1.1, 3.5.1.2, 3.5.1.3, 3.6.1, 3.6.1.1, 3.6.1.2, 3.6.1.3, 3.6.1.4, 3.7.1, 3.7.2, 3.7.3, 3.7.4, 3.7.5, 3.7.6, 3.7.7, 3.7.8, 3.7.9, 4.1.1, 4.2.1, 4.2.1.1, 4.2.1.2, 4.2.2, 8.3.2, 12.3.3
18. AICPA SOC 2 TSC: CC6.7, PI1.2, PI1.4, PI1.5

## Document ownership

<(Choose from)>

* 1. Policy Owner:
     1. [Owner name] ([Owner email]), [Owner title]
  2. Information Security Officer:
     1. [Information officer name], ([Information officer email]), [Information officer title]
  3. System Owner(s):
     1. [System owner name], ([System owner email]), [System owner title]
  4. Process and Operational Owner(s)
     1. [process owner], ([process owner email]), [process owner title]
  5. System Administrator(s):
     1. [System admin name], ([System admin email]), [System admin title]
  6. Required Dissemination: <(Choose from)>
     1. IT Administrator
     2. Engineering
     3. Product Management
     4. Support
     5. Information Security Team
     6. [Organization name] Leadership Team
     7. Contractors
     8. Vendors
     9. Company Wide
     10. [Organization name] SIRT
  7. Optional Dissemination: <(Choose from)>
     1. IT Administrator
     2. Engineering
     3. Product Management
     4. Support
     5. Information Security Team
     6. [Organization name] Leadership Team
     7. Contractors
     8. Vendors
     9. Company Wide
     10. [Organization name] SIRT

## Purpose

The purpose of this Cryptography Policy is to ensure the confidentiality, integrity, and availability of sensitive and confidential information through the use of strong cryptographic controls. This policy aims to protect data at rest and in transit, manage cryptographic keys securely, and comply with industry standards and regulatory requirements. By implementing encryption practices, this policy seeks to mitigate risks associated with data breaches, unauthorized access, and other cyber threats.

## Scope

This policy applies to all employees, contractors, vendors, and third-party entities who access, manage, or handle the organization's sensitive or confidential information. It encompasses all data storage, transmission, and communication processes, including but not limited to:

* Encryption of data at rest on all storage media and devices.
* Encryption of data in transit across internal and external networks.
* Protection of communication sessions and wireless network traffic.
* Management of cryptographic keys, including key creation, storage, rotation, and disposal.
* Administration of public keys
* Procedures for incident response in the event of compromised or lost keys.

This policy covers all information systems, applications, and network infrastructure owned, operated, or managed by the organization, ensuring comprehensive protection of all digital assets.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], [owner title] | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | Executive Team | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | Executive Team | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], [Information officer title] | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner],  Operational owner title] |  |
| Information Systems Administrators | System Administrators | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], [HR title] | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users | End Users | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | [provider type] | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
  2. Management has reviewed and approved this policy.
  3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
  4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
  2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. AES-256: Advanced Encryption Standard, a symmetric encryption algorithm used for secure data encryption.
  2. Asymmetric Encryption: A type of encryption that uses a pair of keys (a public key and a private key) for encryption and decryption.
  3. Cryptographic Key: A string of characters used within a cryptographic algorithm to transform plaintext into ciphertext or vice versa.
  4. Data at Rest: Data that is stored physically on any digital medium (e.g., databases, spreadsheets, archives, backups).
  5. Data in Transit: Data actively moving from one location to another, such as across the internet or through a private network.
  6. FIPS: Federal Information Processing Standards, which are publicly announced standards developed by the United States federal government for use in computer systems.
  7. Hardware Security Module (HSM): A physical device that manages digital keys and provides cryptographic processing.
  8. Key Management: The process of handling cryptographic keys, including their generation, exchange, storage, use, and replacement.
  9. PKI (Public Key Infrastructure): A framework for managing digital certificates and public-key encryption.
  10. RSA-2048: A public-key encryption algorithm using a 2048-bit key size, often used for securing data transmission.
  11. Session Hijacking: An attack where a user session is taken over by an attacker.
  12. Symmetric Encryption: An encryption method where the same key is used to both encrypt and decrypt the data.
  13. TLS: Transport Layer Security, a cryptographic protocol designed to provide secure communication over a computer network.
  14. WPA3: Wi-Fi Protected Access 3, a security protocol used to protect wireless networks.
  15. Wireless Network Traffic: Data that is transmitted over a wireless network.

## Policy

#### Data at Rest

The [responsible party] shall:

* + 1. Encrypt all sensitive or confidential data stored on company-owned or company-provided systems, devices, media, etc.
    2. Implement encryption for whole disks, partitions/files, disk drives, backups, and databases using AES-256 or equivalent encryption standards​​.

#### Data in Transit

The [responsible party] shall:

* + 1. Protect the authenticity and confidentiality of communication sessions using strong cryptographic methods​​.
    2. Implement session management controls to prevent session hijacking and ensure session integrity​​.
    3. Ensure all sensitive or confidential data in transit is encrypted using TLS 1.2 or higher​​.
    4. Encrypt data transmitted over public networks and internal communication channels​​.

#### Wireless Network Traffic and Wireless Devices

The [responsible party] shall:

* + 1. Ensure that all wireless network communications are encrypted using WPA3 or equivalent standards​​.
    2. Disable wireless networking capabilities when not in use and enforce strong authentication mechanisms for all wireless connections​​.

#### Key Creation

The [responsible party] shall:

* + 1. Generate cryptographic keys using FIPS-compliant random number generators​​.
    2. Ensure keys are of adequate length and complexity, e.g., 256-bit for symmetric keys and 2048-bit for asymmetric keys​​.

#### Key Storage

The [responsible party] shall:

* + 1. Store cryptographic keys in hardware security modules (HSMs) or other secure key management systems​​.
    2. Protect keys against unauthorized access and disclosure​​.

#### Key Rotation

The [responsible party] shall:

* + 1. Implement regular key rotation policies, with a minimum rotation period of one year for encryption keys​​.
    2. Establish expiration dates for keys
    3. Ensure all key changes are documented and managed securely​​.

#### Public Keys

The [responsible party] shall:

* + 1. Use public key infrastructure (PKI) to manage public keys for APIs​​.
    2. Ensure public key certificates are issued, renewed, and revoked according to a defined certificate policy​​.
    3. Securely distribute and store public keys to prevent unauthorized access and tampering​​.
    4. Assign unique keys to identified accounts

#### Incident Response

The [responsible party] shall:

* + 1. Immediately revoke and replace any compromised or lost cryptographic keys​​.
    2. Notify affected parties and take steps to mitigate any potential damage caused by the compromise​​.
    3. Conduct a thorough investigation to determine the cause of the key compromise and implement measures to prevent future incidents​​.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
  2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
  3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
     1. Policies
     2. Procedures
     3. Standards
     4. Documentation
     5. Regulations
     6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
  2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
     1. The Information Security Officer
     2. Officer of the [Organization name] Leadership Team
  3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |