Insert the organization logo by clicking on the image icon

Encryption Policy Template

Date:

**Document Control**

|  |  |
| --- | --- |
| **Document Title:** | Encryption Policy Template |
| **Document ID:** |  | Version: | 0.1 |
| **Status:** | Draft |  |
| **Publish Date:** |  |

**Document Review**

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Reviewer(s) | Remarks |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Objective 4](#_Toc97455977)

[2. Scope 4](#_Toc97455978)

[3. Policy 4](#_Toc97455979)

[3.1 General Requirements 4](#_Toc97455980)

[3.2 Safe Use of Encryption 5](#_Toc97455981)

[3.3 Encryption key management 5](#_Toc97455982)

[4. Other Requirements 6](#_Toc97455983)

[5. Policy Enforcement 7](#_Toc97455984)

# Objective

The purpose of this policy is to provide cyber security requirements based on best practices and standards to ensure the proper and effective use of encryption to protect the electronic information assets of <entity name> and to reduce cyber risks and internal and external threats by focusing on the basic objectives of protection, namely: confidentiality, integrity and availability of information.

# Scope

This policy covers all electronic information assets of <entity name>, and applies to all employees of <entity name>, including the entities you deal with and third parties.

# Policy

## General Requirements

1. The <entity name> shall develop, document, and approve coding procedures and standards based on the work need and on the risk analysis in the <entity name>. These procedures include the approved encryption solutions and the restrictions applied to them (technically and organizationally), the methods of using them, the mechanism for issuing, publishing, and restoring keys, in addition to managing backup copies of keys and procedures for destroying encryption keys.
2. Data during transmission and storage shall be encrypted based on its classification and according to the regulatory policies and procedures of <entity name>, and relevant legislative and regulatory requirements.
3. Updated methods, algorithms, keys, and encryption devices must be used according to best practices and standards issued in this regard.
4. All sensitive systems data must be encrypted during Data-In-Transit.
5. All sensitive systems data must be encrypted during storage (Data-at-Rest) at the file level, the database, or at the level of specific columns within the database.
6. Roles must be defined and documented, and responsibilities related to the management of the cryptographic keys infrastructure (Key Management Infrastructure "KMI”), for at least the following roles:
* Keys and Encryption Administration: Responsible for keys and encryption systems (Keying Material Manager) as <Director of the Department for Cyber Security>.
* Cryptographic administrators responsible for protecting cryptographic keys (Key Custodians).
* Certification authorities “CAs” so that they are reliable and secure.
* Registration authorities concerned with registering, so that they are reliable and secure.

## Safe Use of Encryption

1. All cryptographic solutions used (including algorithms, programs, modules, libraries and other cryptographic components) must be identified, evaluated, and approved by <Department Concerned with Cyber Security> prior to their implementation in <entity name>.
2. Must ensure that the encryption is applied according to the encryption solutions approved by <entity name>.
3. The use of internally developed encryption algorithms is prohibited according to the Open Web Application Security Project (OWASP) cryptographic guide.
4. Secure verification methods (such as use cryptographic public keys, digital signatures, and digital certificates) to reduce risks according to the encryption solutions approved in <entity name>.
5. User identity verification shall be used to transfer highly confidential data to third parties using approved digital certificates, and in accordance with the data and information protection policy approved in <entity name>.
6. You must use a verification method from identity Multiple Items (Multi-Factor Authentication “MFA”) to verify the user’s authority to access sensitive systems in accordance with the data and information protection policy approved by <entity name>.

## Encryption key management

1. Cryptographic keys must be managed in a secure manner throughout their lifecycle operations (Key Lifecycle Management) and ensure that they are used properly and efficiently.
2. Cryptographic certificates must be issued by the internal certificate authority at <entity name> for on-premises services or by a trusted third party.
3. Private key information must be kept in a safe place (especially if it is used for electronic signature), preventing unauthorized access, including certificate authorities.
4. Techniques must be provided to protect encryption keys when stored (Tamper Resistant Safe).
5. Private keys must be protected by securing them by a password and/or by storing it on a secure medium, in accordance with approved encryption procedures.
6. Private encryption keys must be classified as "Top Secret" information in accordance with the data classification policy adopted at <entity name>.
7. Event logs for cryptographic key management solutions should be enabled and monitored periodically.
8. A term for using encryption keys, a creation date, and an expiration date must be specified for each key.
9. Encryption keys must be renewed before they expire.
10. Updated Certificate Revocation List must be used to ensure that expired or compromised encryption certificates are not used in future transactions.
11. In the event that the private key used by <entity name> is exposed to a security breach or if the key is not available (due to damage to the key storage media), the certificate authority must be notified immediately to cancel it and re-issue the encryption key (The private key).
12. The concerned authority must be obligated to issue certificates, in the event that their encryption keys (Private) were exposed Keys. To a security breach, report <entity name> and immediately revoke all certificates and replace the private key of the certificate authority.
13. In the event that keys cannot be exchanged securely and reliably across telecommunication networks, encryption keys must be transmitted using alternative, secure and independent out-of-band channels.
14. Encryption key length requirements should be reviewed and updated Based on the latest relevant technical developments, at least once a year and in compliance with national coding standards.
15. Cryptographic maintainers are responsible for protecting the cryptographic keys (Key Custodians) and are only authorized to replace cryptographic keys when needed.
16. It is forbidden to save encryption keys to the main memory or to keep them on the same systems on which the encryption is applied. Instead, it is recommended that they be stored on stand-alone devices (Peripheral Hardware Devices), such as Cryptographic Key Protection Devices (Hardware Security Modules “HSM”), Key Storage Systems (Key Loaders), or any other devices designated for this purpose.

# Other Requirements

* 1. Cybersecurity requirements for encryption should be reviewed periodically.
	2. This policy should be reviewed once a year; at least.

# Policy Enforcement

1. Policy document sponsor and owner: <Head of Cyber Security Department>.
2. Policy implementation and enforcement: <Department Concerned with Information Technology>.
3. Any violation of this policy may subject the offender to disciplinary action as per the procedures followed in <entity name>.

-End of the Document-