This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the outlined image.

Cryptography Policy Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously
- Enter “<organization name>” in the Find text box
- Enter your organization’s full name in the “Replace” text box
- Click “More”, and make sure “Match case” is ticked
- Click “Replace All”
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated by	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This policy aims to define the cybersecurity requirements related to cryptography to protect the <organization name>'s electronic technology assets in order to achieve the primary purpose of reducing cybersecurity risks resulting from internal and external threats in the <organization name>.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to (ECC-1:2018), (CSCC-1:2019), (NCS-1:2020) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This policy covers all <organization name>'s information and technology assets and applies to all personnel (employees and contractors) In the <organization name>, including stakeholders and third parties.

Policy Requirements

1 General Requirements

1-1 <organization name> must develop, document, and approve procedures, standards and controls for cryptography based on business need and analysis of risks present in the <organization name> where the security level complies with (NCS-1:2020) issued by the NCA.

1-2 Information must be encrypted during transmission and storage based on their classification and as per <organization name>'s policies and regulatory procedures as well as relevant legal and regulatory requirements.

1-3 Up-to-date and secure algorithms and their methods must be applied during cryptography in accordance with relevant legal and regulatory requirements.

1-4 Data and information transferred to or from cloud services must be encrypted in accordance with relevant legal and regulatory requirements.

1-5 Data-in-transit must be encrypted for all critical systems.

1-6 Data-at-Rest must be encrypted for critical systems at files level, database, or at the level of specific columns within database.

1-7 Cryptography cybersecurity requirements must be reviewed periodically in <organization name>.

1-8 Key performance indicators must be used to ensure the continuous improvement and effective and efficient use of the cryptography requirements.

2 Use of Cryptography

2-1 Cryptography solutions used (including algorithms, software, modules, libraries, and other cryptographic components) by cybersecurity function in <organization name> must be listed, evaluated and approved before applying them in <organization name>.

2-2 Implementation of cryptographic fundamentals used (e.g., Symmetric algorithms and Asymmetric algorithm) must be ensured as per (NCS-1:2020).

2-3 Implementation of cryptography as per <organization name>'s cryptographic solutions must be ensured.

2-4 Internally developed cryptography algorithms must not be used, as per OWASP's "Guide to Cryptography" and NCS-1:2020.

2-5 Secure authentication methods (e.g. using public keys, digital signatures, and digital certificates) must be used in accordance with <organization name>'s cryptographic solutions to reduce cybersecurity risks.

2-6 User authentication must be used to transfer highly confidential data to third parties using approved digital certificates, and in accordance with <organization name> data and information protection policy and its compliance with legal and regulatory requirements.

2-7 Cryptographic standard controls must be defined into two levels of cryptographic standard controls strength, moderate and advanced levels, in order to ensure flexibility and efficiency of implementation as per NCS-1:2020.

2-8 Cryptography techniques used in the OT/ICS networks environment must be compatible with NCS-1:2020.

2-9 Up-to-date and secure cryptography methods and algorithms must be used upon creation, saving, and transfer, and on the entire network connection used to transfer data classified as confidential and highly confidential according to the advanced level as per DCC-1:2021.

2-10 Up-to-date and secure cryptography methods and algorithms must be used upon creation, saving, and transfer, and on the entire network used to transfer data classified as confidential and highly confidential according to the moderate level as per DCC-1:2021.

2-11 Up-to-date and secure methods, algorithms, keys, and cryptography devices must be applied at the advanced level when using cloud services as per CCC-1:2020.

2-12 Up-to-date and secure cryptography methods and algorithms must be used on the entire telework network as per the advanced level within NCS and TCC-1:2021.

2-13 Use of cryptographic designs and methods (such as block cypher, MAC, AEAD, etc.) must be ensured as per NCS-1:2020.

3 Common Cryptographic Protocols

3-1 Use of cryptographic protocols such as IPSEC and TLS must be ensured and taken into account as per NCS-1:2020.

3-2 Use of acceptable versions of protocols in (Remote Safe Connection, Bluetooth, Universal Mobile Telecommunications System (UMTS/LTE/5G) and WIFI secure access) must be ensured as per NCS-1:2020.

4 PKI

4-1 Use of PKI certification algorithms must be ensured as per NCS-1:2020.

4-2 Validity of the certificates used must be ensured as per NCS-1:2020.

4-3 Data and information used with keys must be securely managed.

4-4 Roles and responsibilities related to PKI management must be limited to at least the following roles:

4-4-1 Keying Material Manager as <Cybersecurity Director>.

4-4-2 Key custodians are the only ones authorized to substitute keys when necessary.

4-4-3 Certification Authorities (CAs) that are reliable and secure.

4-4-4 Registration Authorities (RAs) are reliable and secure.

5 Key Cycle Management

5-1 Keys must be managed securely during Key Lifecycle Management Processes while ensuring their proper and effective use as per <organization name> cryptographic standard controls.

5-2 Cryptographic certificates must be issued by the <Internal Certification Authority> in the <organization name> for local services or by a trusted third party.

5-3 Private keys must be kept in a safe place (especially if used for digital signatures) and unauthorized access to such keys, including by the certification authorities, must be prohibited.

5-4 Tamper resistant safe for storing keys must be provided.

5-5 Private keys must be safeguarded by locking with a password and/or by storing on secure media as per <organization name> cryptographic standard controls.

5-6 Key Lifecycle Management Processes requirements must be adhered to for each process within the key lifecycle from creation until its destruction as per the <organization name> cryptographic standard controls such as:

- Key Generation
- Key Registration/Certification
- Key Use
- Key Storage
- Key Revocation/Validation
- Key Archive
- Key Destruction
- Key Accounting

5-7 Private keys must be classified as "Top Confidential" information as per <organization name> data and information classification policy.

5-8 Prohibit saving cryptographic keys in main memory or systems subject to cryptography; instead they must be saved in other devices (e.g. Hardware Cryptographic Modules (HCM), Key Storage, or other devices dedicated for this purpose.

5-9 Limited lifetime from creation time to expiry time for cryptographic keys must be defined.

5-10 Cryptographic keys must be renewed before their expiry.

5-11 Up-to-date copy of certificate revocation list must be used to ensure that expired or compromised certificates are not used in future transactions.

5-12 If a private key used by <organization name> is compromised or if the key is unavailable (because of damage to key storage media), the issue must be immediately reported to the certification authority to revoke it and reissue user private key.

5-13 If the certification authority private key has been compromised, <organization name> must be informed, all certificates must be immediately revoked, and the certification authority private key must be replaced.

5-14 In case secure key exchange is not possible over communication networks, cryptographic keys must be transmitted using out-of-band channels.

5-15 Cryptographic key length requirements must be reviewed and updated at least annually and in line with NCS-1:2020.

Roles and Responsibilities

1- **Policy Owner:** <head of the cybersecurity function>

2- **Policy Review and Update:** <cybersecurity function>

3- **Policy Implementation and Execution:** <IT Function>

4- **Policy Compliance Measurement**: <cybersecurity function>

Update and Review

<cybersecurity function> must review the policy at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this policy on a regular basis.

2- All personnel at <organization name> must comply with this policy.

3- Any violation of this policy may be subject to disciplinary action as per <organization name>'s procedures.