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 Standard 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 entity 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 standard aims to define the detailed cybersecurity requirements related to the cryptography of <organization name> to achieve the main objective which is minimizing cybersecurity risks resulting from internal and external threats.

The requirements in this standard are aligned with the Cryptography Policy and the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This standard covers all <organization name>'s systems, applications and processing devices and applies to all personnel (personnel and contractors) in the <organization name>.

Standards

1	Use of Cryptography
Objective	To ensure that the use of cryptography is securely managed and used appropriately when required.
Risk Implication	If cryptography is not used properly and as necessary, this can have severe implications that could lead to information theft, unauthorized access, and information disclosure.
Requirements	
1-1	Valid Transport Layer Security (TLS) certificates must be used for all sensitive information in transit between the client, server and other servers
1-2	TLS certificates must be obtained from a recognized Certificate Authority (CA) for all production services at <organization name>.
1-3	Internet browsers must be configured to avoid insecure and weak protocols (e.g., SSLv3 or SSLv2), and weak ciphers (e.g., DES or MD5) while ensuring to use protocols with

	alignment with the National Cryptography Standards (NCS-1:2020).
1-4	Encrypted channels must be used for all authentications.
1-5	It must be ensured that backups are properly protected via physical security and encryption when they are stored and moved across the network. Such backups must include remote backups and cloud services.
1-6	All network devices must be managed using encrypted sessions.
1-7	During a cryptographic process, if an error is detected in the received information, and the receiver requires that the information be entirely correct (e.g., the receiver cannot proceed when the information is in error), then the following must be performed: • The information must not be used. • The recipient may request that the information be resent (retransmissions must be limited to a predetermined maximum number of times). • Information related to the incident must be stored in an audit log to later identify the source of the error.
1-8	The strength levels must be designed to target a 128-bit security level for the basic level and a 256-bit security level for the advanced level as per the National Cryptographic Standard (NCS-1:2020).
2	Data and Information Encryption
Objective	To ensure that data and information is encrypted when necessary.
Risk Implication	Unencrypted data and information has severe implications that could lead to information theft, unauthorized access, and information disclosure.

Requirements	
2-1	Approved whole disk encryption software must be used to encrypt the hard drive of all mobile devices.
2-2	All encrypted network traffic must be decrypted at the boundary proxy prior to analyzing the content. However, <organization name> may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.
2-3	All remote login access to <organization name>'s network must be required to encrypt data in transit.
2-4	All traffic leaving <organization name> must be monitored, and any unauthorized use of encryption must be detected.
2-5	If USB storage devices are used, data stored on such devices must be encrypted while at rest, based on the data classification.
2-6	All protected information in transit must be encrypted.
2-7	All protected information at rest must be encrypted using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.
2-8	All wireless data in transit must be encrypted.
2-9	All authentication credentials must be encrypted or hashed with a salt when stored
2-10	It must be ensured that all account usernames and authentication credentials are transmitted across networks using encrypted channels.
2-11	Servers storage media must be encrypted, including hard disks, Network Attached Storage (NAS), Storage Area Network (SAN) connected storage, or any other type of connected storage.

2-12	Databases must be encrypted to prevent unauthorized access to data classified as confidential, secret, and top secret.
2-13	Data must be transmitted over the network and between systems using encryption mechanisms strong enough to minimize the risk of data exposure.
2-14	Database files, on the database-level or field-level, must be encrypted as per <organization name>'s relevant policies and procedures.
2-15	Backup tapes that store backups must be encrypted, and the key must not be stored in the same tapes in plain text.
2-16	All administrator, user or application traffic to and from the DBMS must be encrypted.
2-17	End-to-end encryption for web applications client/server communications must be implemented.
3	Other Cryptographic Related Information
Objective	To ensure that data and information used in conjunction with keys is securely managed.
Risk Implication	Insecure management of data and information used in conjunction with cryptographic keys has severe implications that could lead to information theft, unauthorized access, and information disclosure.
Requirements	
3-1	All information used in conjunction with cryptographic algorithms and keys must be protected.
3-2	Associations for cryptographic information must be protected according to their type.
3-3	An assurance of domain parameter validity must be obtained for all discrete log public key algorithms to ensure that the domain parameters are arithmetically correct, using one of the following methods:

	• Assurance from the key owner, key verifier, or trusted third party • Explicit validation depending on the algorithm used
3-4	Non-cryptographic mechanisms must be incorporated in communication systems to ensure the availability of transmitted cryptographic information after it has been successfully received, rather than relying on retransmission by the original sender for future availability.
4	Cryptographic algorithms and schemes
Objective	To ensure that approved and secure cryptographic algorithms and schemes are used when using cryptography.
Risk Implication	Use of insecure or unapproved cryptographic algorithms and schemes has severe implications that could lead to information theft, unauthorized access, and information disclosure.
Requirements	
4-1	Only cryptographic hash functions must be used to ensure that it is not feasible to find a message that produces a given hash value (Pre-image Resistance) or find two messages that produce the same hash value (Collision Resistance).
4-2	Accepted cryptographic hash functions should be used based on national cryptographic standards (NCS-1:2020).
4-3	Key lengths that are at least 128 bits must be used in all symmetric key algorithms.
4-4	Message Authentication Codes (MACs) must be used to provide assurance of the data's integrity, and that the MAC was computed by the expected organization.
4-5	Only MAC algorithms must be used based on block cipher algorithms (CMAC) or based on hash functions (HMAC).
4-6	The same key must not be used if the same block cipher algorithm is used for both encryption and MAC computation.

4-7	Approved digital signature algorithms must be used to provide source authentication, integrity authentication, and support for non-repudiation.
4-8	Only the following digital signature algorithms must be used with the approved key sizes for each of the following: • Digital Signature Algorithm (DSA) • RSA Algorithm • ECDSA Algorithm • Merkle
4-9	Digital signatures must be generated using keys that meet or exceed the approved key sizes of the algorithm.
4-10	Only the following approved key-exchange scheme types must be used to set up keys between communicating entities: • Key Transport: The keying material must be transported from one organization to another using a symmetric algorithm (i.e., using a key-wrapping key), or using an asymmetric algorithm. • Key Agreement: Entities must co-create shared keying material using symmetric or asymmetric algorithms.
4-11	Approved key-exchange schemes with approved key sizes must be used. These schemes include Diffie-Hellman (DH) and RSA algorithms and Elliptic Curve Diffie-Hellman (ECDH) for the advance level.
4-12	Security strengths of at least 256 bits must be employed for cryptographic algorithms used for critical systems as per the National Cryptographic Standard (NCS-1:2020).
4-13	Security strengths of at least 256 bits must be employed for hash functions used for critical systems.
4-14	Authenticated Encryption with Associated Data (AEAD) and the accepted schemes must be used such as:

	• Galois Counter Mode (GCM) • Counter with CBC-MAC (CCM)
4-15	When using Hybrid Encryption Schemes the accepted schemes must be used such as: • Elliptic Curve Integrated Encryption Scheme (ECIES) • Discrete Logarithm Integrated Encryption Scheme (DLIES) • RSA with Optimal Asymmetric Encryption Padding (RSA-OAEP)
5	Commonly Used Cryptographic Protocols
Objective	To ensure that approved and secure cryptographic protocols are used when using cryptography.
Risk Implication	Use of insecure or unapproved cryptographic protocols has severe implications that could lead to information theft, unauthorized access, and information disclosure.
Requirements	
5-1	IP Security algorithms must be used for authentication, and must use the Authentication Header (AH) and encapsulation security payload (ESP) with authentication designs of (MAC) such as but not limited to: HMAC-SHA2-384, HMAC-SHA3-256.
5-2	Acceptable versions of the Transport Layer Security (TLS) protocol must be used such as TLS 1.2 and TLS 1.3
5-3	Domain Name System Security (DNSSEC) must be used and the accepted requirements for both zone data signing and message authentication such as ECDSA_P384_SHA-384 and HMAC_SHA- 384.
5-4	Acceptable secure remote connection protocol versions and requirements must be used such as SSH-2 and AEAD_AES_128_GCM.

5-5	Acceptable version and requirements must be used for Bluetooth such as Bluetooth 4.1, Security Mode 4 and AES-CCM.
5-6	Acceptable requirements of the UMTS / 4G (LTE) / 5G system must be used such as: • For Universal Mobile Telecommunications System (UMTS), UEA1-128 must be used with UA1-128. • For 4G (LTE), must use 128-EEA2 with 128-EIA2. • For the fifth generation (5G),must use OR 128-NEA2 with 128-NIA2.
5-7	Acceptable versions of Wi-Fi Protected Access (WPA) must be used such as WPA3-Enterprise.
5-8	Kerberos Protocol must use the accepted requirements for both basic and advance level such as: • (CAMELLIA128-CTS-CMAC) • (AES256-CTS-HMAC-SHA3)
5-9	Server management protocol that supports encryption or configures encryption for server management protocols, such as LDAP over TLS, SNMPv3 with authentication and privacy, Kerberos with TLS, encrypted syslog, etc., must be used.
5-10	Encryption for server application and database communication protocols, such as HTTPS, Secure API, TDE or SQL with TLS, SFTP, SSHv2, etc., must be configured.
5-11	Unencrypted protocols or non-secure services (such as HTTP, FTP, etc.), must not be used, and HTTPS, SFTP, etc. must be used instead.
5-12	Encryption technologies, such as Transport Layer Security (TLS) and Virtual Private Networks (VPN), must be implemented to protect authentication mechanisms during transmission.

5-13	Web application protocols must be configured to use encryption wherever applicable (e.g., HTTPS, SFTP over TLS, etc.).
5-14	The use of secure encrypted management protocols such as Secure Shell (SSH) v2 and Remote Desktop Protocol (RDP) over TLS must be restricted.

Roles and Responsibilities

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

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

3- **Standard Implementation and Execution:** <information technology organization>

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

Update and Review

<cybersecurity function> must review the standard at least once a year or in case any changes occur in the infrastructure or 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 standard on a regular basis.

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

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