



# Cryptography Policy

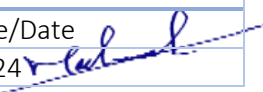
Doc. Control Number	Version
SNL-13	0.3



Document

Reference

Item	Description
Title	Cryptography Policy
Department	Cybersecurity Department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	13 March 2024
Revision-Date	13 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	13/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	13/3/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	13/3/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	16 Jan 2022	Muhaned Ali	First Release
0.2	4 July	Muhaned Ali	The policy has been reviewed
0.3	13 March 2024	Muhaned Ali	The policy has been reviewed



## Contents

1. Purpose.....	4
2. Scope.....	4
3. Policy.....	4
4. Roles and Responsibilities.....	6
5. Compliance and Enforcement.....	6
6. Policy Review .....	7

## 1. Purpose

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards to ensure the proper and effective use of encryption to protect SNLC's electronic information assets and to reduce cyber risks and internal and external threats by focusing on the primary objectives of protection: confidentiality, integrity, and availability of information.

## 2. Scope

This policy covers all SNLC's electronic information assets and applies to all SNLC employees, including its transactors and third parties.

## 3. Policy

### 3.1 General clauses

- a) The SNLC shall develop, document, and approve cryptographic procedures and standards based on the business need and risk analysis of the SNLC and such that the security level complies with the CST, and Aramco.
- b) Data must be encrypted during transmission and storage based on its classification and as per SNLC regulatory policies and procedures, and relevant legislative and regulatory requirements.
- c) SNLC must implement encryption mechanisms, using at least AES encryption algorithm, and 256 bits key, on all devices or storage media hosting sensitive data per the SNLC's assets classification policy.
- d) Operating system images installed on desktop and laptop computers must be configured with a minimum of AES 256 bit (Advanced Encryption Standard).
- e) During the build process for desktops and laptops, processes must be in place to check the make and model of computers to verify they have a Trusted Platform Module (TPM) chip on board.

### 3.2 Basic Cryptographic Protocols and Techniques

- a) The following cryptographic protocols and techniques are approved for use within SNLC:
  - AES 256 (Advanced Encryption Standard with a key size of 256 bits)
  - RSA 2048 (Rivest-Shamir-Adleman encryption algorithm with a key size of 2048 bits)
  - PKI (Public Key Infrastructure) for digital certificates and key management.

### 3.3 Relevant Restrictions

- a) Self-Signed Certificates: The use of self-signed certificates should be avoided whenever possible. Certificates issued by trusted Certificate Authorities (CAs) are preferred.
- b) MD5 (Message Digest 5): The use of MD5 for cryptographic hashing is strictly prohibited due to its vulnerability to collision attacks. Hash functions such as SHA-256 (Secure Hash Algorithm 256-bit) should be used instead.

### 3.4 Cryptographic Solutions List

Cryptographic Solution	Compliance with Restrictions	Risk Assessment	Approval Status
AES 256-bit	Legal: Yes, Technical: Yes	Low Risk	Approved
RSA 2048-bit	Legal: Yes, Technical: Yes	Medium Risk	Approved
SHA-256 (Hash Function)	Legal: Yes, Technical: Yes	Low Risk	Approved
TLS 1.3 (Protocol)	Legal: Yes, Technical: Yes	Low Risk	Approved
X.509 Digital Certificates	Legal: Yes, Technical: Yes	Medium Risk	Approved



Diffie-Hellman Key Exchange	Legal: Yes, Technical: Yes	Medium Risk	Approved
Self-Signed Certificates	Legal: NO, Technical: NO	High Risk	Not Approved
MD5 (Hash Function)	Legal: NO, Technical: NO	High Risk	Not Approved

### 3.5 Application of Approved Cryptographic Protocols

#### a) **Data in Transit:**

- All sensitive data transmitted over public or untrusted networks shall be encrypted using approved cryptographic protocols.
- When accessing company systems remotely, use SSH for secure shell access.
- For secure file transfers, utilize FTPS (FTP Secure) to encrypt your data.
- Accessing web-based services and applications must be done through HTTPS.
- Ensure that all communications between networked systems are secured using TLS.
- When applicable, use IPSEC to secure communication at the network layer.

#### b) **Data at Rest:**

- Sensitive data stored on electronic media or devices shall be encrypted using approved cryptographic algorithms.
- Encryption should be applied to data stored in databases, file systems, backup archives, and removable storage media.

#### c) **Data in Use:**

- Sensitive data being processed or used by applications or users shall be protected using appropriate cryptographic techniques.
- The use of secure containers, hardware security modules (HSMs), and virtual private networks (VPNs) may be employed to protect data during processing.

### 3.6 Secure use of encryption

- a) All cryptographic solutions used (including algorithms, programs, modules, libraries, and other cryptographic components) must be identified, evaluated, and approved by the Information Security Department prior to their implementation in SNLC.
- b) Ensure that encryption is applied according to SNLC-approved encryption solutions.
- c) Secure verification methods (such as the use of cryptographic public keys, digital signatures, and digital certificates) should be used to reduce cyber risks and in accordance with SNLC-approved encryption solutions.
- d) User identity verification shall be used to transfer highly confidential data to third parties using approved Digital Certificates, and in accordance with the SNLC Approved Data and Information Protection Policy.
- e) A Multi-Factor Authentication ("MFA") method must be used to verify the user's eligibility to access sensitive systems in accordance with the SNLC Data and Information Protection Policy.

### 3.7 Encryption key management

- a) Cryptographic keys must be managed securely throughout Key Lifecycle Management and ensure that they are used properly and efficiently.
- b) Cryptographic certificates must be issued by SNLC's internal certificate authority for on-premises services or by a trusted third party.



- c) The private key information must be kept in a safe place (especially if it is used for electronic signature), preventing unauthorized access, including to certificate authorities.
- d) Techniques to protect encryption keys when they are stored (Tamper Resistant Safe) must be provided.
- e) Private Keys must be protected by securing them with a password and/or by storing them on a secure medium, according to approved encryption procedures.
- f) Private encryption keys must be classified as "top secret" information in accordance with the SNLC Data Classification Policy.
- g) Event logs for cryptographic key management solutions must be enabled and monitored periodically.
- h) For each key, a term to use encryption keys, a creation date, and an expiration date must be specified.
- i) Encryption keys must be renewed before they expire.
- j) An updated Certificate Revocation List should be used to ensure that expired or compromised encryption certificates are not used in future transactions.
- k) If the private encryption key used by SNLC has been compromised or the key is not available (due to corruption of the key storage media), the certificate authority must be notified immediately to revoke it and re-issue the private key.
- l) If a security breach occurs, the certificate authority must notify SNLC, immediately revoke all certificates and replace the certificate authority's private key.
- m) If keys cannot be exchanged securely and reliably across telecommunication networks, encryption keys must be transmitted using alternative, secure, and independent out-of-band channels.
- n) Cryptographic 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 cryptographic standards.
- o) Cryptographic maintainers are responsible for protecting the cryptographic keys (Key Custodians) and are only authorized to replace cryptographic keys when needed.
- p) It is forbidden to save encryption keys to the main memory or to keep them in the same systems on which the encryption is applied. Instead, it is recommended that they be stored on separate devices (Peripheral Hardware Devices, such as Hardware Security Modules "HSM"), Key Storage Systems (Key Loaders), or any other devices designated for this purpose.

#### 4. Roles and Responsibilities

- 4.1 The sponsor and owner of the policy document: Head of Cyber Security Department.
- 4.2 Policy reviews and update: Cyber Security Department.
- 4.3 Policy implementation: IT Department & Cyber Security Department.

#### 5. Compliance and Enforcement

- 5.1 Compliance with this policy is mandatory for all employees and individuals working with information assets within SNLC.
- 5.2 Non-compliance with this policy may result in disciplinary action, including but not limited to retraining, suspension, termination, and legal consequences, as appropriate.



## 6. Policy Review

6.1 This policy will be reviewed on a periodic basis to ensure its continued relevance and effectiveness. Any updates or modifications to this policy shall be communicated to all relevant employees and stakeholders.