Encryption Standard Model

Doc. Control Number	Version
SNL-46	0.2

Document Reference

Item	Description
Title	Encryption Standard Model
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	28 May 2024
Revision-Date	28 May 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/28/2024

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/28/2024

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/28/2024

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	28 May 2023	Muhaned Ali	First Release
0.2	28 May 2024	Muhaned Ali	The document has been reviewed

Contents

1. Purpose

The purpose of this standard is to provide cyber security requirements based on best practices and standards related to encryption for SNLC to reduce cyber risks and protect them from internal and external threats by focusing on the basic objectives of protection, namely: information confidentiality, integrity, and availability. It must also comply with the National Cryptographic Standards issued by the National Cyber Security Authority as a basic reference with the highest priority for cyber security requirements for encryption.

This standard aims to comply with cybersecurity requirements and related legislative and regulatory requirements. It is a legislative requirement in Control No. 2-8-1 of the Basic Cybersecurity Controls (ECC-1:2018) issued by the National Cybersecurity Authority.

2. Scope

This standard covers all systems, applications, and information processing devices of SNLC, and applies to all employees of SNLC.

3. List of Cryptographic solutions

Cryptographic solutions	Technique	Regulations
Remote access with FortiGate FW	IPsec VPN	Comply with ISO/27001, Aramco, and NCA
ERP transaction over the internet	Symmetric encryption using TLS (Asymmetric techniques used to share session key)	Comply with ISO/27001, Aramco, and NCA
SSH protocol is used to securely operate network services.	RSA 512	Comply with ISO/27001, Aramco, and NCA
Data storage on devices	Encrypt all data at rest Windows 10, 11, and Windows Server. By using BitLocker - AES 128 bits, or 256 bits	Comply with ISO/27001, Aramco, and NCA
Email security using Google workspace encryption	Symmetric/asymmetric encryption using S/MIME	Comply with ISO/27001, Aramco, and NCA

- SNLC Used the Cryptographic Solutions listed above to safeguard data during its entire life cycle (in transit, at rest, and in use). According to IT Asset Management policy.

4. Standards

1	Use of Cryptography
Purpose	Ensure encryption is managed and used securely and appropriately when required.
The potential risks	Failure to use encryption appropriately and when necessary, can lead to serious risks of information theft, disclosure, or unauthorized access.
Required Procedures	
1-1	Valid Transport Layer Security (TLS) certificates shall be used for all sensitive information in transit between the client, server, and other servers.
1-2	TLS certificates shall be obtained from a recognized Certificate Authority (CA) for all production services at SNLC.
1-3	Internet browsers shall be configured to avoid insecure and weak protocols (e.g., SSLv3 or SSLv2), and weak ciphers (e.g., DES or MD5).

1-4	Encrypted channels shall be used for all authentications.
1-5	It shall be ensured that backups are properly protected via physical security and encryption when they are stored and moved across the network. Such backups shall include remote backups and cloud services.
1-6	All network devices shall 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 shall be performed: • The information shall not be used. • The recipient may request that the information be resent (retransmissions shall be limited to a predetermined maximum number of times). • Information related to the incident shall be stored in an audit log to later identify the source of the error.
2	**Cryptographic Key Management**
Purpose	Ensure that cryptographic keys are managed securely during the complete cryptographic key management cycle.
The potential risks	Managing insecure encryption keys carries a high risk of information theft, disclosure, or unauthorized access.
Required Procedures	
2-1	Cryptographic keys shall be managed in accordance with SNLC's cryptographic key management processes, procedures, and guidelines. This shall include key generation, key storage, key backup, key recovery, etc.
2-2	Cryptographic keys shall be categorized according to their classification (public, private, or symmetric) and use.
2-3	Cryptographic keys shall be protected according to their type and the required protection.
2-4	Associations for the cryptographic keys shall be protected according to their type.
2-5	An assurance of public-key validity shall be obtained to ensure that the cryptographic key is arithmetically correct, through one of the following methods: • Assurance from the key owner, key verifier, or trusted third party. • Explicit public key validation depending on the algorithm used.
2-6	Algorithms that provide an assurance of private-key possession shall be used. Alternatively, such assurance shall be obtained explicitly to ensure that the external entity (i.e., third party) providing a public key possesses the associated private key.
2-7	The security protections highlighted in control 2-2 shall be provided for a period as per the cryptographic key type.

2-8	Cryptoperiods shall be assigned to the cryptographic keys.
2-9	All symmetric keys and all private keys shall be destroyed at the end of their period of protection as highlighted in control 2-6.
2-10	Cryptographic key lengths that are at least 128 bits shall be used in all symmetric key algorithms.
2-11	Asymmetric cryptosystem keys that are of sufficient length shall be used to yield equivalent strength to symmetric key lengths.
2-12	For critical systems, it is recommended to employ symmetric cryptographic key lengths that are at least 256 bits, and asymmetric Elliptic Curve Cryptography ECC key lengths that are at least 512 bits.
3	Data and Information Encryption
Purpose	Ensuring data and information encryption when necessary.
The potential risks	Unencrypted data and information carry a significant risk of theft, disclosure, or unauthorized access to information.
Required Procedures	
3-1	Approved whole disk encryption software shall be used to encrypt the hard drive of all mobile devices.
3-2	All encrypted network traffic shall be decrypted at the boundary proxy prior to analyzing the content. However, SNLC may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.
3-3	All remote login access to SNLC's network shall be required to encrypt data in transit and use multi-factor authentication.
3-4	All traffic leaving SNLC shall be monitored, and any unauthorized use of encryption shall be detected.
3-5	If USB storage devices are required, data stored on such devices shall be encrypted while at rest, based on the data classification.
3-6	All protected information in transit shall be encrypted.
3-7	All protected information at rest shall be encrypted using a tool that requires a secondary authentication mechanism not integrated into the operating system, to access the information.
3-8	All wireless data in transit shall be encrypted.

3-9	All authentication credentials shall be encrypted or hashed with a salt when stored.
3-10	It shall be ensured that all account usernames and authentication credentials are transmitted across networks using encrypted channels.
4	Other Cryptographic Related Information
Purpose	Ensure that data and information used with encryption keys are securely managed.
The potential risks	Insecure management of data and information used with encryption keys may lead to significant risks of information theft, disclosure, or unauthorized access.
Required Procedures	
4-1	All information used in conjunction with cryptographic algorithms and cryptographic keys shall be protected.
4-2	Associations for cryptographic information shall be protected according to their type.
4-3	An assurance of domain parameter validity shall 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.
4-4	The security protections highlighted in control 2-2 shall be provided for a period.
4-5	Non-cryptographic mechanisms shall 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.
5	Encryption Protocols and Cipher Suites
Purpose	Ensure that certified and secure encryption algorithms are used when encrypting.
The potential risks	The use of unsecured or unauthorized encryption algorithms carries a significant risk of information theft, disclosure, or unauthorized access.
Required Procedures	
5-1	Only cryptographic hash functions shall 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).
5-2	Cryptographic hash functions shall be used as directed by the relevant algorithm standards.
5-3	Cryptographic key lengths that are at least 128 bits shall be used in all symmetric key algorithms.
5-4	Message Authentication Codes (MACs) shall be used to provide assurance of the data's integrity, and that the MAC was computed by the expected entity.
5-5	Only MAC algorithms shall be used based on block cipher algorithms (CMAC or GMAC) or based on hash functions (HMAC).

5-6	The same key shall not be used if the same block cipher algorithm is used for both encryption and MAC computation.
5-7	Approved digital signature algorithms shall be used to provide source authentication, integrity authentication, and support for non-repudiation.
5-8	Only the following digital signature algorithms shall be used with the approved key sizes for each of the following: • Digital Signature Algorithm (DSA) • RSA Algorithm • ECDSA Algorithm
5-9	Digital signatures shall be generated using keys that meet or exceed the approved key sizes of the algorithm.
5-10	Only the following approved key-exchange scheme types shall be used to set up keys between communicating entities: • Key Transport: The keying material shall be transported from one entity to another using a symmetric algorithm (i.e., using a key-wrapping key), or using an asymmetric algorithm. • Key Agreement: Entities shall co-create shared keying material using symmetric or asymmetric algorithms.
5-11	Approved key-exchange schemes with approved key sizes shall be used. These schemes include Diffie-Hellman (DH) and RSA algorithms.
5-12	Security strengths of at least 256 bits shall be employed for cryptographic algorithms used for critical systems following what the NCA issues in this regard.
5-13	Security strengths of at least 256 bits shall be employed for hash functions used for critical systems.

5. Compliance with the standard

1- The Head of the Cyber Security Department is responsible for ensuring that SNLC adheres to this standard on an ongoing basis.
2- This standard must be complied with by all SNLC employees.
3- Any violation of this standard may result in disciplinary action in accordance with SNLC standards.