Cryptography Policy

MCS Cybersecurity Department

Cybersecurity Management		
Cryptography Policy		
Doc: MCS-CS-POL-08	Issue/Rev: 1.0	Date: 22.12.2024

DOCUMENT VALIDATION & DISTRIBUTION

Prepared By:	Reviewed By	Approved By
Mubashar Rehman NII Consultant Fatmah Mahdi Ahmed Cybersecurity Manager		
Distributed to:		
✓ All Department Manager ✓ General Manager	✓	

REVISION HISTORY

Issue /Rev	Revision Description	Date
1.0	Cryptography Policy	22.12.2024

Cybersecurity Management		
Cryptography Policy		
Doc: MCS-CS-POL-08	Issue/Rev: 1.0	Date: 22.12.2024

TABLE OF CONTENTS

1 ABBREVIATIONS & DEFINITIONS

- **MCS:** Modern Chemicals and Services Company
- **HCIS:** High commission for Industrial security
- **NCA:** National Cybersecurity Authority
- **ECC:** Essential Cybersecurity Controls standard issued by NCA 2018
- **IT:** Information technology
- **CSSC:** Cybersecurity Steering Committee
- **Asset:** Anything tangible or intangible that has value to the organization. There are many types of assets, and some of which include obvious things, such as: persons, machineries, utilities, patents, software, and services. The term could also include less obvious things, such as: information and characteristics (e.g., organization's reputation and public image, as well as skill and knowledge).
- **Penetration Testing:** The practice of testing a computer system, network, web application or mobile application to find vulnerabilities that an attacker could exploit.
- **Cybersecurity:** According to the Royal Decree number 6801, dated 11/2/1439H, cybersecurity is the protection of networks, IT systems, operational technologies systems and their components of hardware and software, their services, and the data they contain, from any penetration, disruption, modification, access, use or unauthorized exploitation. The concept of cybersecurity also includes information security and digital security.
- **Cybersecurity requirements:** It is the cybersecurity requirements which covers in the cybersecurity policy and procedures.
- **ECC-**1:2018: Essential Cybersecurity Controls
- **OTCC-**1:2022:Operational Technology Cybersecurity Controls
- **NCS**-1:2020: National Cybersecurity Standards 2020, issued by NCA
- **DCC**-1:2021: Data Classification Controls 2021 - Guidelines for data classification security levels
- **CCC**-1:2020: Cloud Cryptographic Controls 2020 - Standards for encryption in cloud services
- **TCC**-1:2021: Telework Cryptographic Controls 2021 - Guidelines for encryption in remote work environments
- **OT/ICS:** Operational Technology / Industrial Control Systems - Systems used in industrial and critical infrastructure environments
- **IPSEC:** Internet Protocol Security - A suite of protocols to secure network communications
- **TLS:** Transport Layer Security - A cryptographic protocol ensuring secure communication over networks
- **PKI:** Public Key Infrastructure - A framework for managing digital certificates and encryption keys

- **HCM:** Hardware Cryptographic Module - A physical device used to store and manage cryptographic keys securely
- **Key Lifecycle Management:** The process of managing cryptographic keys from creation to destruction
- **Digital Signature:** A cryptographic mechanism used to verify the authenticity of digital data
- **AEAD:** Authenticated Encryption with Associated Data - A cryptographic method ensuring both confidentiality and integrity
- **MAC:** Message Authentication Code - A cryptographic checksum ensuring message integrity and authenticity
- **Block Cipher:** A method of encrypting data in fixed-size blocks, commonly used in cryptographic systems

2 PURPOSE

This policy aims to define cybersecurity requirements related to MCS's Secure Systems Development Life Cycle (SSDLC) process. The policy intends to set the appropriate requirements to govern MCS's systems and software development process in order to reduce the likelihood of cybersecurity attacks though poorly implemented designs and functionality. Integrating SSDLC good practices with MCS's Information Technology (IT) project and change management processes will help reduce the number, to mitigate the impact and to address the root cause of vulnerabilities in system designs, configurations and software packages.

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 and CSCC-1:2019, in addition to other related cybersecurity legal and regulatory requirements.

3 SCOPE

This policy applies to all MCS systems, applications and software codes that are designed and developed in-house or using third parties, with a target audience of MCS's personnel (employees and contractors).

4 POLICY STATEMENTS

4.1 General Requirements

1- MCS must develop, document, and approve procedures, standards and controls for cryptography based on business need and analysis of risks present in the MCS where the security level complies with (NCS-1:2020) issued by the NCA.
2- Information must be encrypted during transmission and storage based on their classification and as per MCS's policies and regulatory procedures as well as relevant legal and regulatory requirements.

3- Up-to-date and secure algorithms and their methods must be applied during cryptography in accordance with relevant legal and regulatory requirements.
4- Data and information transferred to or from cloud services must be encrypted in accordance with relevant legal and regulatory requirements.
5- Data-in-transit must be encrypted for all critical systems.
6- Data-at-Rest must be encrypted for critical systems at files level, database, or at the level of specific columns within database.
7- Cryptography cybersecurity requirements must be reviewed periodically in MCS.
8- Key performance indicators must be used to ensure the continuous improvement and effective and efficient use of the cryptography requirements.

4.2 Use of Cryptography

1- Cryptography solutions used (including algorithms, software, modules, libraries, and other cryptographic components) by cybersecurity function in MCS must be listed, evaluated and approved before applying them in MCS.
2- Implementation of cryptographic fundamentals used (e.g., Symmetric algorithms and Asymmetric algorithm) must be ensured as per (NCS-1:2020).
3- Implementation of cryptography as per MCS's cryptographic solutions must be ensured.
4- Internally developed cryptography algorithms must not be used, as per OWASP's "Guide to Cryptography" and NCS-1:2020.
5- Secure authentication methods (e.g. using public keys, digital signatures, and digital certificates) must be used in accordance with MCS's cryptographic solutions to reduce cybersecurity risks.
6- User authentication must be used to transfer highly confidential data to third parties using approved digital certificates, and in accordance with MCS data and information protection policy and its compliance with legal and regulatory requirements.
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.
8- Cryptography techniques used in the OT/ICS networks environment must be compatible with NCS-1:2020.
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.
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.

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

4.3 Common Cryptographic Protocols

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

4.4 PKI

1- Use of PKI certification algorithms must be ensured as per NCS-1:2020.
2- Validity of the certificates used must be ensured as per NCS-1:2020.
3- Data and information used with keys must be securely managed.
4- Roles and responsibilities related to PKI management must be limited to at least the following roles:
   - Keying Material Manager as Cybersecurity Manager.
   - Key custodians are the only ones authorized to substitute keys when necessary.
   - Certification Authorities (CAs) that are reliable and secure.
   - Registration Authorities (RAs) are reliable and secure.

4.5 Key Cycle Management

1- Keys must be managed securely during Key Lifecycle Management Processes while ensuring their proper and effective use as per MCS cryptographic standard controls.
2- Cryptographic certificates must be issued by the Internal Certification Authority in the MCS for local services or by a trusted third party.
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.
4- Tamper resistant safe for storing keys must be provided.
5- Private keys must be safeguarded by locking with a password and/or by storing on secure media as per MCS cryptographic standard controls.
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 MCS cryptographic standard controls such as:

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

7- Private keys must be classified as "Top Confidential" information as per MCS data and information classification policy.
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.
9- Limited lifetime from creation time to expiry time for cryptographic keys must be defined.
10- Cryptographic keys must be renewed before their expiry.
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.
12- If a private key used by MCS 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.
13- If the certification authority private key has been compromised, MCS must be informed, all certificates must be immediately revoked, and the certification authority private key must be replaced.
14- In case secure key exchange is not possible over communication networks, cryptographic keys must be transmitted using out-of-band channels.
15- Cryptographic key length requirements must be reviewed and updated at least annually and in line with NCS-1:2020.

5 ROLES AND RESPONSIBILITIES

1- **Policy Owner:** Cybersecurity Manager
2- **Policy Review and Update:** Cybersecurity Department
3- **Policy Implementation and Execution:** IT Department
4- **Policy Compliance Measurement:** Cybersecurity Department

6 UPDATE AND REVIEW

The Cybersecurity Department must review the policy at least once a year or in case any changes happen to the policy or the regulatory procedures in MCS or the relevant regulatory requirements.

7 COMPLIANCE

1- Cybersecurity Manager will ensure the compliance of MCS with this policy on a regular basis.
2- All personnel of MCS must comply with this policy.
3- Any violation of this policy may be subject to disciplinary action according to MCS's procedures.

8 REFERENCES

- ECC – 2: 2024 2-8-1 Cryptography