Data Cybersecurity Policy

MCS Cybersecurity Department

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	Data Cybersecurity Policy	20.12.2024

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
- **BYOD:** Bring Your Own Device, A policy allowing employees to use their personal devices (e.g., smartphones, laptops) for work purposes
- **KPI:** Key Performance Indicator, A metric used to evaluate the effectiveness of an organization in achieving key business objectives
- **Data Leakage Prevention (DLP):** Technology or solutions that monitor and prevent data from being leaked or transferred outside of the organization's control
- **Cryptography:** The practice and study of techniques for secure communication, ensuring data confidentiality, integrity, and authentication
- **Data Classification:** The process of categorizing data based on its sensitivity and importance to the organization, ensuring proper handling and protection
- **Telework Systems:** Systems used to facilitate remote working, such as virtual private networks (VPNs), cloud services, and secure communication platforms
- **Social Media Accounts:** Online platforms used by the organization for marketing, communication, and engagement with the public

2 PURPOSE

This policy aims to define the cybersecurity requirements related to the data cybersecurity in MCS to achieve the main objective of this policy which is minimizing cybersecurity risks resulting from internal and external threats at MCS in order to preserve confidentiality, integrity and availability.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) 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 comply with the laws and regulations pertaining to data protection in the Kingdom of Saudi Arabia; and MCS policies and procedures.
2- MCS must set and update, on a regular basis, data cybersecurity requirements.
3- MCS must ensure data cybersecurity requirements is managed efficiently in accordance with the MCS's Cybersecurity in Human Resources Policy and Asset Management Policy.
4- MCS must ensure the protection of mobile devices as per the MCS's mobile devices security policy.
5- MCS must use Data Leakage Prevention technology/solutions.
6- MCS must prohibit the use of MCS's data in any environment other than the production environment, except after conducting a risk assessment and applying controls to protect that data, such as: data masking or data scrambling techniques.
7- MCS must identify the techniques, tools and procedures for the implementation of secure data disposal according to the classification level.
8- MCS must develop and implement exist strategy to ensure means for secure disposal of data on termination or expiry of the contract with the cloud service provider.
9- MCS must ensure the proper and efficient use of cryptography techniques to protect MCS's data as per the approved MCS's cryptography policy and standard, and related laws and regulations.
10- MCS must identify roles and responsibilities to ensure data cybersecurity in relevance with legal and regulatory requirements.
11- MCS must use secure means to export and transfer data and virtual infrastructure.

12- MCS must prohibit the transfer of any critical systems data from production environment to any other environment.

13- MCS must use watermark feature to label the whole document when creating, storing, printing, or displaying the document on the screen, and making sure each copy of the document has a traceable number.

14- Key performance indicators (KPI) must be used to ensure the continuous improvement and effective and efficient use of cybersecurity requirements for data protection.

4.2 Classification and Secure Handling of Information

1- MCS's data must be classified according to the approved MCS Data Classification Policy.

2- All MCS's data must be classified in all formats:
- Digital (such as word documents, spreadsheets, presentations and databases).
- Electronic communications (such as email messages, voice communication services and teleconferencing).
- Physical (such as printouts, hard copies of contracts and notebooks).
- Spoken (such as meetings, interviews and phone calls).

3- Individuals must avoid discussing MCS's data in spoken formats in public areas, or in areas they might be overheard. Spoken discussions should occur in MCS premises and in secure locations within the premises.

4- All data held by MCS on all systems (including critical systems) and cloud systems must be classified and labelled according to all relevant legal and regulatory requirements, as well as the approved Data Classification policy in MCS.

5- Data owners appointed by MCS, working with the relevant stakeholders within MCS, must be responsible for classifying data as described in this policy.

6- Any violation of this policy and data classification controls must be reported to the relevant stakeholders within of MCS immediately.

7- Remote access controls on data must be enforced and implemented as per MCS's identity and access management policy.

8- Classified data (Secret, Top secret) must not be stored on portable storage devices such as external hard drives or USB sticks, regardless of the level of encryption used on the portable storage device.

9- Classified data (Top secret, Secret) must not be input, processed, changed, stored or transmitted on employee-owned devices —termed Bring Your Own Device (BYOD)—, unless that data is the data of the employee.

10- Classified data (e.g., Secret, Top secret), that can be accessed, processed, stored or transmitted through telework systems must be protected.

11- The subset of classified data (e.g., Secret, Top secret), that can be accessed, processed, stored or transmitted through telework systems must be identified in accordance with the relevant regulations.

12- Technology assets for management of MCS's social media accounts must not contain classified data, as per relevant regulations.

4.3 Retention of records

1- MCS must retain records of consent given by data owners and must retain records of withdrawal or revocation of consent for the length of time specified by law or regulation.

2- MCS must keep a record of all secure data disposal operations that have been executed.

3- MCS must retain data for the length of time specified by law or regulation or until the sensitive information is no longer required for the purpose for which it was collected.

4- MCS must create a record of processing activities, update it when required and retain copies for the length of time specified by law or regulation.

5- Identifying retention period for all systems-associated data, in accordance with relevant legislations. Only required data must be retained in the production environment.

5 ROLES AND RESPONSIBILITIES

1- **Policy Owner:** Cybersecurity Manager

2- **Policy Review and Update:** Cybersecurity Department

3- **Policy Implementation and Execution:** Information Technology Department and Cybersecurity 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 2-7-1 Data and Information Protection