Cybersecurity Management		
Compliance with Cybersecurity Legislation and Regulations Policy		
Doc: MCS-CS-POL-05	Issue/Rev: 1.0	Date: 20.12.2024

Compliance with Cybersecurity Legislation and Regulations Policy

MCS Cybersecurity Department

Cybersecurity Management		
Compliance with Cybersecurity Legislation and Regulations Policy		
Doc: MCS-CS-POL-05	Issue/Rev: 1.0	Date: 20.12.2024

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	Compliance with Cybersecurity Legislation and Regulations Policy	20.12.2024

Cybersecurity Management		
Compliance with Cybersecurity Legislation and Regulations Policy		
Doc: MCS-CS-POL-05	Issue/Rev: 1.0	Date: 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
- **CSCC:** Critical Systems Cybersecurity Controls
- **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

2 PURPOSE

This policy aims to define the cybersecurity compliance requirements for MCS. 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 covers all systems and procedures in the MCS and applies to all personnel (employees and contractors) in the MCS.

4 POLICY STATEMENTS

4.1 General Requirements

1- Define and document a list of local and international legislation and regulations related to cybersecurity and relevant requirements applicable to MCS on a continuous basis once changed or once new requirements are issued. Should there be any locally approved international agreements or obligations that include cybersecurity requirements, they must be added to the list.
2- Comply with all local and international legislation and regulations, as well as clauses of cybersecurity agreements and obligations, that apply to MCS.
3- Provide the necessary technologies to verify compliance with the requirements of legal and regulatory authorities related to cybersecurity.
4- Review cybersecurity policies and procedures with cybersecurity legislation and contract clauses annually.
5- Monitor compliance of external service providers with cybersecurity legislation and contract clauses on a continuous and permanent basis.
6- Ensure implementation of cybersecurity policies and procedures annually.
7- Ensure compliance with requirements related to cybersecurity through the use of appropriate tools, including but not limited to:
   - Cybersecurity Risk Assessment activities.
   - Vulnerability Management activities.
   - Penetration Test activities.
   - Review of cybersecurity standards.
   - Security Source Code Review.
   - User surveys.
   - Stakeholder interviews.
   - Review of privileges on the system and network.
   - Review of cybersecurity logs and events.
8- Define and implement the necessary corrective measures to correct the gaps for all compliance requirements by stakeholders.
9- Implement appropriate procedures to ensure compliance with legal and regulatory requirements, related to intellectual property rights and the use of software.
10- MCS Cybersecurity Function must review the implementation of Cybersecurity Controls on a regular basis.
11- Cybersecurity Function must review the implementation of Critical Systems Cybersecurity Controls at least once a year.
12- Review and audit implementation of cybersecurity controls in MCS by parties that are independent from the Cybersecurity Function (such as the <internal audit function> at MCS). Review and audit must be carried out independently, taking into account the

principle of non-conflict of interests, as per the general standards accepted for review and auditing as well as the relevant legal and regulatory requirements.

13- Document and present the results of cybersecurity review and audit to the cybersecurity steering committee and representative of parties independent from cybersecurity function (e.g. <internal audit function> in the MCS). As well, results must also include the scope of review and audit, observations, recommendations and corrective measures, as well as feedback remediation plan.
14- Review CSCC implementation by parties independent of the cybersecurity function from MCS at least once a year.
15- Use KPI in a proper and effective manner to ensure continuous improvement and proper and effective use of cybersecurity compliance program requirements.

5 ROLES AND RESPONSIBILITIES

1- **Policy Owner:** Cybersecurity Manager
2- **Policy Review and Update:** Cybersecurity Department
3- **Policy Implementation and Execution:** 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- The 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 1-7-1 Compliance with Cybersecurity Standards, Laws and Regulations