



Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Cybersecurity Risk Management Policy			
Doc: MCS-CS-POL-14	Issue/Rev: 1.0	Date: 22.12.2024	

Cybersecurity Risk Management Policy

MCS Cybersecurity Department

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات</div><div>Modern Chemicals & Services Company</div></div>
Cybersecurity Risk Management Policy			
Doc: MCS-CS-POL-14	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	Cybersecurity Risk Management Policy	22.12.2024

Cybersecurity Management			<div><div>MCSO</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Cybersecurity Risk Management Policy			
Doc: MCS-CS-POL-14	Issue/Rev: 1.0	Date: 22.12.2024	

TABLE OF CONTENTS

1	ABBREVIATIONS & DEFINITIONS	4
2	PURPOSE	5
3	SCOPE.....	5
4	POLICY STATEMENTS	5
4.1	GENERAL REQUIREMENTS	5
4.2	MAIN STAGES FOR CYBERSECURITY RISKS MANAGEMENT	6
4.2.1	<i>Risk Identification</i>	6
4.2.2	<i>Risk Assessment:</i>	6
4.2.3	<i>Risk Response:</i>	7
4.2.4	<i>Risk Oversight:</i>	7
4.3	RISK APPETITE.....	8
4.4	CYBERSECURITY RISKS IN OT/ICS	8
5	ROLES AND RESPONSIBILITIES.....	9
6	UPDATE AND REVIEW	9
7	COMPLIANCE	9
8	REFERENCES	9

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Cybersecurity Risk Management Policy			
Doc: MCS-CS-POL-14	Issue/Rev: 1.0	Date: 22.12.2024	

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
- **ISO:** International Organization for Standardization
- **ISO27005:** ISO standard for Information Security Risk Management
- **ISO31000:** ISO standard for Risk Management Guidelines
- **Quantitative:** A risk analysis method that uses numerical values to assess risks
- **Qualitative:** A risk analysis method that uses descriptive assessments (e.g., likelihood, impact) rather than numerical values
- **NIST:** National Institute of Standards and Technology
- **ERM:** Enterprise Risk Management
- **KPI:** Key Performance Indicator
- **DCC:** Data Cybersecurity Controls
- **Operational Technology (OT):** Hardware and software used to monitor or control physical processes in industries such as manufacturing

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات</div><div>Modern Chemicals & Services Company</div></div>
Cybersecurity Risk Management Policy			
Doc: MCS-CS-POL-14	Issue/Rev: 1.0	Date: 22.12.2024	

2 PURPOSE

This policy aims to define the cybersecurity requirements related to MCS's cybersecurity risk management to achieve the main objective of this policy which is minimizing cybersecurity risks resulting from internal and external threats at 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 legal and regulatory requirements.

3 SCOPE

This policy covers all information and technology assets and systems in the MCS in addition to its work procedures in MCS and applies to all personnel (employees and contractors) in the MCS.

4 POLICY STATEMENTS

4.1 General Requirements

- 1- Cybersecurity Risk Management Methodology and cybersecurity risk management procedures in MCS must be defined, documented and approved, while ensuring its alignment with the National Cybersecurity Risk Management Framework, which has already been aligned with internationally approved standards and guidelines (e.g. ISO27005, ISO31000, NIST).
- 2- The Cybersecurity Risk Management Methodology must serve the following purposes:
 - Define, collect, and list assets, then classify and prioritize them based on the level of protection required.
 - Define and evaluate risks to the business, assets, or personnel of MCS (e.g. cybersecurity risks on MCS).
 - Evaluate cybersecurity risks in planning and before approving use of social media as well as telework for any service or system.
 - Define and evaluate information and technology assets vulnerability to specific threats.
 - Define decisions to respond to such risks.
 - Prioritize risk response plans based on specific procedures.
 - Classify and define risk levels based on the risk probability and impact on MCS.
 - Define the roles and responsibilities to manage and deal with cybersecurity risk.
- 3- A periodic risk assessment must be conducted to ensure security of information and technology assets and prioritization of risk levels.
- 4- Cybersecurity risks must be managed in a methodological approach to protect information and technology assets in MCS.
- 5- Cybersecurity risks in MCS must be managed and overseen on a continuous basis.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات</div><div>Modern Chemicals & Services Company</div></div>
Cybersecurity Risk Management Policy			
Doc: MCS-CS-POL-14	Issue/Rev: 1.0	Date: 22.12.2024	

- 6- Cybersecurity Risk Management must be aligned with the Enterprise Risk Management “ERM” in MCS.
- 7- Risk management related recommendations, issued by NCA, must be applied.
- 8- Key performance indicators (KPI) must be used to ensure the continuous improvement and effective and efficient use of Cybersecurity Risk Management requirements.

4.2 Main Stages for Cybersecurity Risks Management

4.2.1 Risk Identification

This process must cover the following:

- 1- Assets must be identified and an inventory list must be prepared with prioritized list and classifications.
- 2- Potential vulnerabilities and threats on assets must be identified.
- 3- Current risks on assets must be identified through:
 - Developing potential risks scenarios as per the identified vulnerabilities, threats and attacks.
 - Identifying currently applied cybersecurity controls to counter identified risks.

4.2.2 Risk Assessment:

- 1- The Cybersecurity Department must implement cybersecurity risk assessment procedures as a minimum in the following cases:
 - Every 3 years at least for all information and technology assets, and at least once a year for critical systems, telework systems, and social media accounts.
 - At early stages of technology projects.
 - Before making major changes to infrastructure.
 - When planning to acquire new services from a third party.
 - At the planning stage and before the launch of new technology products and services.
- 2- Risks must be re-assessed and updated as follows:
 - After a cybersecurity incident that compromises information and technology asset integrity, availability, or confidentiality.
 - After a significant audit findings or proactive data.
 - Whenever information and technology assets experience significant enhancement or modification.
- 3- Current risks assessment process must cover the following:
 - **Risk Analysis:** The MCS must assess the likelihood of threats, assess their consequences and use results to determine the overall risk level. The MCS

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات</div><div>Modern Chemicals & Services Company</div></div>
Cybersecurity Risk Management Policy			
Doc: MCS-CS-POL-14	Issue/Rev: 1.0	Date: 22.12.2024	

must adopt a Quantitative or Qualitative methodology to conduct risk analysis.

- **Risk Evaluation:** The MCS must evaluate cybersecurity risk against its adopted enterprise risk evaluation criteria in the MCS to prioritize such risks.

4.2.3 Risk Response:

- 1- The MCS must select the risk response decision based on the following:
 - **Risk Mitigation:** Mitigate or reduce risk degree by applying the necessary security controls to reduce the likelihood or impact or both, which help control risks and bring them to a level that could be accepted. The organization must do the following:
 - Identifying, documenting and prioritizing risk response plans to deal with current risks.
 - Executing risk response plans based on priority.
 - Calculating residual risks after conducting risk response plans.
 - **Risk Avoidance:** Remove risk by avoiding the conditions that create it.
 - Risk Transfer: Pass the risk to a third party that has better capabilities to deal with it or insure information and technology assets against cybersecurity risks.
 - Risk Acceptance: Risk level is acceptable but in MCS continuous monitoring is required in case of any change.
- 2- Risk treatment options must be selected and documented based on the outcomes of risk assessment, cost of implementation and expected benefits.

4.2.4 Risk Oversight:

- 1- To oversee risks, MCS must develop and maintain a risk register to document outcomes of risk management process. This must include at a minimum the following information:
 - Risk identifier.
 - Scope of risks.
 - Risk Owner.
 - Description of risks including their causes and impacts.
 - Risk analysis highlighting risk consequences and their timescale.
 - Risk evaluation and rating covering risk likelihood and magnitude and overall risk rating if the risk occurs.
 - Risk treatment plan covering risk treatment action, owner, timeline.
 - Residual risk description.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات</div><div>Modern Chemicals & Services Company</div></div>
Cybersecurity Risk Management Policy			
Doc: MCS-CS-POL-14	Issue/Rev: 1.0	Date: 22.12.2024	

- 2- Cybersecurity risk register must be created for operations, cloud computing services, and critical systems and periodically oversee it in alignment with the risk profile.
- 3- Cybersecurity risks related to telework systems, services and systems allowed to work remotely, social media accounts, and the services and systems used must be included in the organization cybersecurity risk register and oversee them at least once a year.
- 4- The MCS must collect and review guides related to cybersecurity risks state on an annual basis.
- 5- Risk management reports must be developed.

4.3 Risk Appetite

- 1- Criteria for risk appetite must be defined and documented as per risk level and cost of treatment compared to impact.
- 2- Risk appetite level must be defined for cloud computing services.
- 3- If a residual risk does not match the criteria of risk appetite, further controls to reduce risks to an acceptable level must be applied.
- 4- If a residual risk does not match the criteria of risk appetite, further controls to reduce risks to an acceptable level must be applied.

4.4 Cybersecurity risks in OT/ICS

- 1- OT/ICS cybersecurity risk methodology must be developed as part of risk management methodology and safety risk management and procedures adopted in MCS.
- 2- OT/ICS cybersecurity risks must be evaluated periodically along with the risks of signing contracts and agreements with external parties concerned with OT/ICS and /or when changes to relevant legal and regulatory requirements occur , as part of the assessment.
- 3- A cybersecurity risk register related to OT/ICS must be included in the risk register of MCS.
- 4- Appropriate levels of areas and facilities containing OT/ICS must be defined based on an approved methodology.
- 5- A qualitative analysis of cybersecurity risks must be included in the Process Hazard Analysis procedures, which applies to any change in processes, procedures, or factories.
- 6- In the event that the cybersecurity requirements cannot be met within the OT/ICS environment, the necessary justifications must be clarified and documented, approved by the Cybersecurity Department and also approved by the representative.
- 7- If cybersecurity risk appetite is approved, alternative controls must be identified, documented and approved by the representative and reviewed by the Cybersecurity

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Cybersecurity Risk Management Policy			
Doc: MCS-CS-POL-14	Issue/Rev: 1.0	Date: 22.12.2024	

Department to make sure they are effectively and timely implemented, while assessing and reviewing those risks on a continuous basis.

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 1-5-1 Cybersecurity Risk Management