



Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Cybersecurity Incident and Threat Management Policy			
Doc: MCS-CS-POL-11	Issue/Rev: 1.0	Date: 22.12.2024	

Cybersecurity Incident and Threat Management Policy

MCS Cybersecurity Department

Cybersecurity Management			<div> الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div>
Cybersecurity Incident and Threat Management Policy			
Doc: MCS-CS-POL-11	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 Incident and Threat Management Policy	22.12.2024

Cybersecurity Management			<div> الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div>
Cybersecurity Incident and Threat Management Policy			
Doc: MCS-CS-POL-11	Issue/Rev: 1.0	Date: 22.12.2024	

TABLE OF CONTENTS

1	ABBREVIATIONS & DEFINITIONS	4
2	PURPOSE	4
3	SCOPE.....	5
4	POLICY STATEMENTS	5
4.1	GENERAL REQUIREMENTS	5
4.2	CYBERSECURITY INCIDENTS REPORTING.....	8
4.3	INCIDENTS RESPONSE AND RECOVERY	8
4.4	THREAT INTELLIGENCE FEEDS.....	9
5	ROLES AND RESPONSIBILITIES.....	9
6	UPDATE AND REVIEW	9
7	COMPLIANCE	9
8	REFERENCES	10


Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Cybersecurity Incident and Threat Management Policy			
Doc: MCS-CS-POL-11	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
- **Logs (System/Network Logs):** Recorded data that tracks activities or events occurring within a system or network, often used for monitoring and security purposes.
- **Key Performance Indicator:** A measurable value that demonstrates how effectively an organization is achieving its cybersecurity objectives.
- **Disaster Recovery:** Procedures for recovering critical systems and data following an incident or disaster.
- **Telework:** A working arrangement that allows employees to perform their job duties from a location other than the traditional office, often remotely.
- **Digital Forensics:** The process of collecting, preserving, and analyzing evidence from digital devices in a legally acceptable manner.

2 PURPOSE

This policy aims to define the cybersecurity requirements related to cybersecurity incident and threat management at MCS to minimize cybersecurity risks and protect it against internal and

Cybersecurity Management			<div> الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div>
Cybersecurity Incident and Threat Management Policy			
Doc: MCS-CS-POL-11	Issue/Rev: 1.0	Date: 22.12.2024	

external threats by focusing on key security objectives namely; confidentiality, integrity, and availability.

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 (TCC-1:2021), in addition to other related cybersecurity legal and regulatory requirements.

3 SCOPE

This policy covers all information and technology assets in the MCS and applies to all personnel (employees and contractors) in the MCS.

4 POLICY STATEMENTS

4.1 General Requirements

- 1- The MCS must establish the required mechanisms to timely identify and detect cybersecurity incidents in MCS to effectively manage reports received from personnel or beneficiaries.
- 2- The MCS must proactively handle cybersecurity incidents by adopting defensive mechanisms to prevent or mitigate the impacts on confidentiality, integrity, or availability.
- 3- Incident response plan must be documented and approved to establish procedures to address any cyber-attack, defining response team roles and responsibilities, defining decision making authority, and establishing interaction mechanism with internal and external stakeholders as well as incident escalation plan.
- 4- Cybersecurity incident response capabilities, readiness level, and approved plan must be tested periodically through Attack Simulation Exercises.
- 5- Provide organization's personnel (employees and contractors) with the required skills and training to effectively respond to cybersecurity incidents.
- 6- Examples of cybersecurity Incidents shall include but not limited to:
 - Unauthorized changes in workstations configurations – both desktops and/or laptops and server's configurations.
 - Malware infections.
 - Changes in applications in terms of appearance (unusual appearance) in addition to modifications in user's privileges
 - Unauthorized access to data or modification of data without authorization or user's privileges.
 - Attempts to gain information that may be used to initiate an attack (Port Scans, Social Engineering attacks, targeted scans across IP range, etc.).
 - Unauthorized activation of suspended or deleted user accounts.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات</div><div>Modern Chemicals & Services Company</div></div>
Cybersecurity Incident and Threat Management Policy			
Doc: MCS-CS-POL-11	Issue/Rev: 1.0	Date: 22.12.2024	

- 7- Cybersecurity incident response plans must be aligned with the IT incident response plans, crisis management and business continuity plans.
- 8- In case of telework, cybersecurity incident response plans and contact information must be updated within the organization in line with the status of telework, ensuring communication capability and readiness of incident response teams
- 9- In case a cybersecurity incident is detected in MCS, the incident response team must immediately take the necessary steps to handle the detected incident by analysing the incident data and determining its impact.
- 10- If a cybersecurity incident is detected, relevant available information such as system and network logs, logs from relevant security products (e.g. logs from malware protection solutions, firewall, and advanced intrusion detection and prevention protection systems) must be analysed.
- 11- Necessary evidence (e.g. evidence collection in accordance with legal constraints and evidence protection against unauthorized tampering) must be handled, documented and maintained securely to preserve its merits. Such evidence must be analysed without damage or modification to its original form.
- 12- In case a cybersecurity incident is detected, the cause of cybersecurity incident must be investigated, supported by specialists, such as digital forensics analysts and cyber incident response teams.
- 13- The incident response plans, capabilities and readiness, must be reviewed at least once a year.
- 14- Cybersecurity incidents must be classified according to severity level and impact on MCS's business
- 15- Cybersecurity incidents must be classified according to the relevant legal and regulatory requirements as per the table below:

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Cybersecurity Incident and Threat Management Policy			
Doc: MCS-CS-POL-11	Issue/Rev: 1.0	Date: 22.12.2024	

TABLE 1: CYBERSECURITY INCIDENTS CLASSIFICATION

Severity Level	Definition	Target Response Time	Target Incident Resolution Time
Catastrophic	Catastrophic failures of services or negative impact on national cybersecurity that result in or threaten to cause serious economic or social complications or lead to death of certain people.	<To be determined by organization> Immediate	<To be determined by organization> Immediate
Critical Incident	Gross threat or damage to image, reputation or credibility of MCS, multiple business functional units getting severely impacted, location of business critically affected, and business continuity measures would have to be invoked.	Immediate	<To be determined by organization> 2 hours
High Incident	Severe outage affecting single business functional units, key services or location.	<To be determined by organization> 1-2 Hours	<To be determined by organization> 4-5 hours
Medium Incident	Moderate degradation to business functional units, locations, IT assets in addition to moderate to high impact to non-critical business units within in MCS.	<To be determined by organization> 2-3 hours	<To be determined by organization> 8-9 hours
Limited Incident	Affecting few resources and the issue can be tolerated for a particular period of time.	<To be determined by organization> 5 hours	<To be determined by organization> 24 hours

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Cybersecurity Incident and Threat Management Policy			
Doc: MCS-CS-POL-11	Issue/Rev: 1.0	Date: 22.12.2024	

16- Key performance indicators (KPI) must be used to ensure the continuous improvement as well as proper and effective use of Cybersecurity Incident and Threat Management requirements.

4.2 Cybersecurity Incidents Reporting

- 1- Raise security awareness of MCS's personnel and define their cybersecurity incidents and threats responsibilities to promptly report any cybersecurity incident or threat.
- 2- The MCS must establish point of contact (POC) for reporting incidents internally, be it a phone number or email address.
- 3- The MCS must specify which incident or threat to be reported, when and to whom they are reported. The parties most commonly notified include, Cybersecurity Manager , incident response teams within the MCS, and information and technology assets owners.
- 4- Prior to disclosure of information about security incidents to third parties, approvals must be obtained according to the relevant legal and regulatory requirements.
- 5- Report cybersecurity incidents to NCA once detected.
- 6- Share incident reports and breach indicators and reports with NCA.

4.3 Incidents Response and Recovery

- 1- Incident response team in MCS must create a detailed cybersecurity incident report. The report must include incident type and category, personnel who reported it, tools used in detecting the incident, service/assets/information affected, how they were detected, and any relevant supporting documents.
- 2- Analyse and update Root Cause Analysis of cybersecurity incidents and develop plans to address them.
- 3- If needed, involve vendors to resolve the incident and/or restore the service.
- 4- Implement and execute cybersecurity incident and threat recommendations and alerts issued by the sector supervisor or NCA.
- 5- Cybersecurity incident recovery procedures must identify vulnerabilities exploited and apply the necessary remediation technical and administrative measures, including but not limited to
 - Implement compensating controls.
 - Deploy updated security patches.
 - Restore system backup versions.
 - Reconfigure security devices including firewalls and intrusion detection systems.
- 6- The MCS must safeguard incident reports (which includes data about security intrusions and incidents such as information about individuals, organizations, specific systems and/or attack methodology) and restrict access to it.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Cybersecurity Incident and Threat Management Policy			
Doc: MCS-CS-POL-11	Issue/Rev: 1.0	Date: 22.12.2024	

- 7- The incident, if not resolved and corrected within the pre-defined timeframes, must be escalated as per the classification of security incidents and incidents escalation rules and procedures.
- 8- Any changes to technology components required to resolve an incident, must be performed in accordance with the MCS's Change Management Process.
- 9- The incident response team at MCS must hold a "lessons learned" meeting with all involved functions after a major incident to reflect on how to better handle future incidents and how to proactively handle them to prevent or mitigate impacts on MCS's business.

4.4 Threat Intelligence Feeds

- 1- Subscribe with authorized and trusted cybersecurity resources "Threat Intelligence" to collect information about new cybersecurity threats and incidents and act immediately.
- 2- Store and organize the collected threat intelligence feeds in a knowledge base such as wikis which are quite flexible and suitable for developing working notes and indicator metadata.
- 3- Update Intrusion Prevention and Detection Systems to ensure their capability of detecting such threats based on threat intelligence feeds.
- 4- Subscribe with Telework-related threat Intelligence providers with to collect information and deal with such information periodically.

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.

Cybersecurity Management			<div> الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div>
Cybersecurity Incident and Threat Management Policy			
Doc: MCS-CS-POL-11	Issue/Rev: 1.0	Date: 22.12.2024	

8 REFERENCES

- ECC – 2: 2024 2-13-1 Cybersecurity Incident and Threat Management