



Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Physical Security Policy			
Doc: MCS-CS-POL-24	Issue/Rev: 1.0	Date: 21.12.2024	

# Physical Security Policy

## MCS Cybersecurity Department

Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Physical Security Policy			
Doc: MCS-CS-POL-24	Issue/Rev: 1.0	Date: 21.12.2024	

## DOCUMENT VALIDATION &amp; 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	Physical Security Policy	21.12.2024


Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Physical Security Policy			
Doc: MCS-CS-POL-24	Issue/Rev: 1.0	Date: 21.12.2024	

TABLE OF CONTENTS

1	ABBREVIATIONS & DEFINITIONS .....	4
2	PURPOSE .....	4
3	SCOPE.....	4
4	POLICY STATEMENTS .....	5
4.1	GENERAL REQUIREMENTS .....	5
4.2	CONTROLS FOR THE PROTECTION OF AUDIO, COMMUNICATIONS, NETWORK, AND POWER CABLES AGAINST PHYSICAL DAMAGE .....	6
5	ROLES AND RESPONSIBILITIES.....	7
6	UPDATE AND REVIEW .....	7
7	COMPLIANCE .....	7
8	REFERENCES .....	7

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals &amp; Services Company</div></div>
Physical Security Policy			
Doc: MCS-CS-POL-24	Issue/Rev: 1.0	Date: 21.12.2024	

## 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
- **Key Performance Indicator(KPI):** A measurable value that demonstrates how effectively an organization is achieving a business objective.

## 2 PURPOSE

This policy aims to define the cybersecurity requirements related to MCS's physical security in order to minimize cybersecurity risks resulting from internal and external threats at MCS and 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 covers all facilities, information and technology assets, equipment and devices in the MCS and applies to all personnel (employees and contractors) in the MCS.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals &amp; Services Company</div></div>
Physical Security Policy			
Doc: MCS-CS-POL-24	Issue/Rev: 1.0	Date: 21.12.2024	

## 4 POLICY STATEMENTS

### 4.1 General Requirements

- 1- All MCS's physical assets and facilities must be inventoried and classified as per MCS's approved Data and Information Classification Policy.
- 2- Access to critical areas (e.g., data centers, recovery centers, data processing centers, monitoring centers, network communication rooms, and supply areas for devices and technical component) must be controlled and restricted to authorized individuals only.
- 3- Suitable operational procedures must be developed, approved, and applied to grant physical access to MCS's facilities based on the principles of Need-to-know, Need-to-access, and Least Privilege. Moreover, access privileges must be reviewed and audited periodically.
- 4- Detectors of metal and hazardous materials must be used for access to critical areas at MCS.
- 5- Access to and exit from critical areas must be logged, and records must be retained and protected in accordance with MCS's approved Data Protection Cybersecurity Policy.
- 6- Access to and exit from critical areas must be monitored using technologies such as closed-circuit television (CCTV) according to the legal and regulatory requirements approved by MCS, and such access must be monitored continually by specialist personnel.
- 7- Procedures for secure destruction, reuse, and disposal of physical assets containing classified information (including paper documents and storage media) must be developed, and a record of destructed or reused assets must be maintained.
- 8- Infrastructure hardware, in particular storage equipment, must be securely disposed in accordance with the relevant legal and regulatory requirements.
- 9- Security controls must be developed, implemented, and reviewed to protect devices and equipment inside and outside MCS's premises based on their classification.
- 10- Emergency response procedures and evacuation plans for the MCS's buildings and facilities must be developed and implemented in the event of any suspected or actual physical or environmental incidents to ensure the safety of MCS's personnel and critical assets.
- 11- Emergency response procedures and evacuation plans must be reviewed periodically at least once a year.
- 12- Procedures to support and maintain physical assets and equipment must be developed and implemented in accordance with MCS's approved equipment maintenance security standards.
- 13- Cybersecurity security risks must be assessed to detect any security threats, safety threats, and weaknesses that MCS may face and address them to protect information

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals &amp; Services Company</div></div>
Physical Security Policy			
Doc: MCS-CS-POL-24	Issue/Rev: 1.0	Date: 21.12.2024	


assets from being exposed to such threats, as per MCS's approved risk management methodology and the relevant legal and regulatory requirements.

- 14- Physical security capabilities and readiness must be tested <once a year> by conducting simulation drills (e.g., social engineering).
- 15- Attendance of MCS's classified meetings must be restricted to authorized personnel only, and attendees of such meetings must go through security screening and inspection.
- 16- Third parties must only be granted access to MCS's facilities after fulfilling security requirements, and their access must be monitored. They must be escorted wherever required for the duration of their presence.
- 17- Physical access management privileges must be restricted to personnel with specific privileges and must be audited and reviewed periodically in accordance with MCS's approved Identity and Access Management Policy.
- 18- Access, storage, and transmission of backup content of critical systems and media must be secured and protected against unauthorized destruction, modification, or access.
- 19- A Clear Desk Policy must be implemented, and documents, information technology devices, or external storage devices must not be left accessible to unauthorized persons.
- 20- Cybersecurity Department must ensure that all personnel have the required knowledge about physical security best practices, such as the duties and responsibilities assigned to them, and ensure their compliance with such practices.
- 21- Physical assets containing classified information must be securely destroyed.
- 22- Key Performance Indicators (KPIs) must be used to ensure the continuous improvement and efficient and effective use of physical security protection requirements.

#### **4.2 Controls for the Protection of Audio, Communications, Network, and Power Cables Against Physical Damage**

Controls must be implemented to protect audio, communications, network, and power cables against physical damage, after examining potential cybersecurity risks. Such controls must cover the following at a minimum:

- 1- Communication and data network cables must be protected against wiretapping.
- 2- Communication and data network cables must not be installed in areas accessible to third parties.
- 3- Communication and data network cables must be protected and isolated securely to protect them against damage or unauthorized interception and ensure that they are installed through secure and protected areas.
- 4- Electrical and power cables must be isolated from communication and data network cables.
- 5- Uninterrupted Power Sources (UPS) must be used to support the continuous operation of critical systems and sites (e.g., data centers).

Cybersecurity Management			<div> الشركة الكيميائية الحديثة للخدمات Modern Chemicals &amp; Services Company</div>
Physical Security Policy			
Doc: MCS-CS-POL-24	Issue/Rev: 1.0	Date: 21.12.2024	

## 5 ROLES AND RESPONSIBILITIES

- 1- **Policy Owner:** Cybersecurity Manager
- 2- **Policy Review and Update:** Cybersecurity Department
- 3- **Policy Implementation and Execution:** Physical Security 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 2-14-1 Physical Security