



Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Storage Media Security Policy			
Doc: MCS-CS-POL-27	Issue/Rev: 1.0	Date: 20.12.2024	

Storage Media Security Policy

MCS Cybersecurity Department

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات</div><div>Modern Chemicals & Services Company</div></div>
Storage Media Security Policy			
Doc: MCS-CS-POL-27	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	Storage Media Security Policy	20.12.2024


Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات</div><div>Modern Chemicals & Services Company</div></div>
Storage Media Security Policy			
Doc: MCS-CS-POL-27	Issue/Rev: 1.0	Date: 20.12.2024	

TABLE OF CONTENTS

1	ABBREVIATIONS & DEFINITIONS	4
2	PURPOSE	4
3	SCOPE.....	4
4	POLICY STATEMENTS	5
4.1	GENERAL REQUIREMENTS	5
4.2	MEDIA ACCESS.....	5
4.3	MEDIA STORAGE	5
4.4	MEDIA TRANSPORT	6
4.5	MEDIA SANITIZATION.....	6
4.6	MEDIA USE.....	6
5	ROLES AND RESPONSIBILITIES.....	6
6	UPDATE AND REVIEW	6
7	COMPLIANCE	6
8	REFERENCES	7

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Storage Media Security Policy			
Doc: MCS-CS-POL-27	Issue/Rev: 1.0	Date: 20.12.2024	

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
- **Network-attached Storage (NAS):** A file-level storage architecture that enables multiple users and devices to access data stored on a centralized server over a network.

2 PURPOSE

This policy aims to define the cybersecurity requirements related to the secure use and disposal of storage media used with MCS's systems, data and information, in order to achieve the main objective of this policy which is minimizing cybersecurity risks 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 MCS's information and technology assets and applies to all personnel (employees and contractors) in MCS.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Storage Media Security Policy			
Doc: MCS-CS-POL-27	Issue/Rev: 1.0	Date: 20.12.2024	

4 POLICY STATEMENTS

4.1 General Requirements

- 1- The MCS must ensure the controlled use of storage media devices utilized to store and transfer information by personnel who have access to information and technology assets at MCS.
- 2- MCS must define what is considered as removable media and which of these can be connected to an information system, computer, or network to provide data storage, such as:
 - Magnetic (e.g., spinning disk drives, tapes).
 - Optical (e.g., optical drives such as CD-R, DVD-R, Blu-ray), and magneto-optical.
 - Semiconductor (e.g., SSD, flash drives, persistent memory devices).
- 3- MCS must prohibit the use of all removable media devices unless a valid business case for its use is provided.
- 4- MCS must design and implement a formal process for approving the use of removable media.
- 5- MCS must physically control and securely store storage media devices within MCS.
- 6- MCS must protect storage media devices until the media are disposed or sanitized using approved equipment, techniques, and procedures, in alignment with the MCS' Secure Disposal Policy.
- 7- MCS must restrict the use and provide secure handling of external storage media.

4.2 Media Access

- 1- Access to the following types of storage media must be restricted in alignment with the Asset Management Policy:
 - Backup Tapes or External Backup Drives
 - Internal Server Storage Drives (HDDs/SSDs)
 - Network-attached storage (NAS) or Cloud Services
- 2- The distribution limitations, handling caveats, and applicable security markings of storage media must be applied.

4.3 Media Storage

- 1- Personnel must be appointed to physically control and securely store media within defined controlled areas.
- 2- Protection of storage media until the media are destroyed or sanitized using equipment approval processes, definition of media handling procedures and approved protection techniques must be ensured.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Storage Media Security Policy			
Doc: MCS-CS-POL-27	Issue/Rev: 1.0	Date: 20.12.2024	

4.4 Media Transport

- 1- Media must be protected and controlled, during transport outside of controlled areas.
- 2- Accountability for storage media during transport outside of controlled areas must be maintained.
- 3- Activities associated with the transport of storage media must be documented and must be restricted to authorized personnel.
- 4- MCS must establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media.
- 5- MCS must review and update the media transportation related policies and procedures at least annually.

4.5 Media Sanitization

- 1- MCS must sanitize storage media prior to its disposal, releasing it out of organizational control or releasing it for reuse using Storage Security Standard in accordance with applicable regulatory and organizational standards and policies.
- 2- Sanitization mechanisms with the strength and integrity commensurate with the classification of the information must be applied.

4.6 Media Use

- 1- MCS must prohibit the use of MCS defined types of storage media on equipment owned by MCS using unapproved security safeguards.

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.

Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Storage Media Security Policy			
Doc: MCS-CS-POL-27	Issue/Rev: 1.0	Date: 20.12.2024	

- 3- Any violation of this policy may be subject to disciplinary action according to MCS's procedures.

8 REFERENCES

- ECC – 2: 2024 2-3-1 Information System and Information Processing Facilities Protection