Cybersecurity Management		
Asset Management Policy		
Doc: MCS-CS-POL-02	Issue/Rev: 1.0	Date: 20.12.2024

Asset Management Policy

MCS Cybersecurity Department

Cybersecurity Management		
Asset Management Policy		
Doc: MCS-CS-POL-02	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	Asset Management Policy	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
- **ERP:** Enterprise Resource Planning
- **CRM:** Customer Relationship Management
- **VPN:** Virtual Private Network
- **CMDB:** Configuration Management Database
- **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
- **Baseline Security Configuration:** A set of minimum security settings applied to an asset to ensure compliance with security policies.
- **Operational Technology (OT):** Hardware and software systems used to detect or control changes in physical processes, such as industrial control systems.
- **Secure Disposal:** The process of permanently and securely disposing of assets, ensuring classified information is wiped before disposal.

2 PURPOSE

This policy aims to define the cybersecurity requirements related to the asset management of MCS's systems, data and information to achieve the main objective of this policy which is minimizing cybersecurity risks resulting from internal and external threats at MCS in order 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 assets (e.g., physical, data, business application, software and technology assets) in MCS and applies to all personnel (employees and contractors) in MCS.

4 POLICY STATEMENTS

4.1 General Requirements

1- All information and technology assets in MCS must be identified and recorded.
2- All information and technology assets in MCS must be in maintained asset inventories and updated annually.
3- Each asset in MCS must have an appointed owner, responsible for the creation, maintenance and accuracy of the asset inventory.
4- All assets in MCS must be configured as per MCS's Secure Configuration and Hardening Policy.
5- All assets must be configured in accordance with published MCS's configuration processes, procedures, standards and guidelines.
6- All asset users and owners must read and sign the asset Acceptable Use Policy approved by MCS before being granted access to any asset.
7- Any breach of the MCS's Acceptable Use Policy may lead to disciplinary action against the individual or individuals breaching the policy. Disciplinary action may include dismissal or termination from MCS.
8- Asset owners must be identified and involved within the asset management lifecycle for critical systems and their components.
9- Key performance indicators must be used to ensure the continuous improvement and effective and efficient use of cybersecurity requirements for asset management.

4.2 Definition of assets

Assets must be grouped into the following types:

1- Classified information asset, which contain classified information as "Top Secret" and "Secret" information (as defined in the MCS's Asset Classification Standard).
2- IT equipment, such as servers, laptops, mobile devices, firewalls, Wi-Fi routers and VPN concentrators, etc.
3- Software and systems, such as:
    - Business applications such as customer relationship management (CRM), enterprise resource planning (ERP), databases and collaboration platforms.

- Software and tools such as operating systems, virtualization software and productivity software.
- Documentation related to critical systems.
- Telework systems and associated assets.

4- Social media accounts and associated assets.
5- Third parties and suppliers and their associated assets.
6- Cloud services providers, cloud computing and hosting providers and managed services and their associated assets.

4.3 Asset ownership

1- In addition to their responsibilities mentioned above, asset owners must be responsible for:
   - Understanding, identifying and managing information risks throughout the information lifecycle.
   - Determining and approving business (including cybersecurity) requirements.
   - Addressing how cybersecurity affects operational technology.
   - Promoting cybersecurity awareness and positive security behaviors.
   - Establishing priorities, budgets and allocating resources.
   - Ensuring information and systems are protected in line with related cybersecurity controls in the organization.
   - Authorizing changes to the assets they control.
   - Supporting cybersecurity reviews and audits.
2- Asset owners must receive a training to enable them to carry out their role and responsibilities.
3- Owners of physical, business applications and software assets must be responsible and not limited to the following:
   - Creating baseline security configurations, obtaining approval, publishing the configurations for the appropriate processes, procedures, standards and guidelines.
   - Implementing the baseline security configurations.
   - Reviewing baseline security configurations at least once a year. If changes are required, owners must update the baseline security configurations, update processes, procedures, standards and guidelines and ensure the changes are implemented using MCS's Change Management Policy.

4.4 Asset inventory

1- An asset inventory must be created for each type of asset as per statement 1-2 in this policy.
2- The asset inventory must be created in electronic format. The asset inventory can be implemented in one of the following examples: Configuration Management Database

(CMDB), asset management software, specialized asset management tool, spreadsheet or database.

3- An asset inventory must be created for all cloud services and information and technology assets related to the cloud services.
4- An asset inventory must be created for critical systems and social media accounts including all information and technology components.
5- Asset inventories must be updated periodically or whenever a change occurs.

4.5 Asset classification and labeling

1- All MCS assets must be classified, labeled and handled in accordance with MCS's policies and related cybersecurity legal and regulatory requirements.
2- Physical assets (network, IT, etc.) must be labeled with a tamper-proof label, stating the unique identification assigned to the asset.
3- Information in digital and paper form must be labeled in accordance with the MCS's Asset Classification Standard.

4.6 Secure disposal

1- All assets owned by MCS must be disposed of in a secure and approved manner as per related legal and regulatory requirements.
2- An Asset Disposal Committee must be established, and it must supervise all disposal activities.
3- The disposal committee must include the asset owner and a representative of the Cybersecurity Department.
4- A secure disposal process for hardware, removable drives, USB devices, software, paper-based records, data, etc. must be defined, approved, and implemented.
5- Classified information stored on an asset must be securely wiped before the asset is disposed.
6- Disposal activities must be recorded and signed by the disposal committee including.
7- The disposal record must include all information about the disposed asset as per MCS's Asset Management Standard, including but not limited to the date, asset type, quantity, label or ID, classification, asset owner, disposal method, etc.

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 employee 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 2-1-1 Asset Management