Cybersecurity Management		
Asset Acceptable Use Policy		
Doc: MCS-CS-POL-01	Issue/Rev: 1.0	Date: 19.12.2024

Asset Acceptable Use Policy

MCS Cybersecurity Department

Cybersecurity Management		
Asset Acceptable Use Policy		
Doc: MCS-CS-POL-01	Issue/Rev: 1.0	Date: 19.12.2024

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 Acceptable Use Policy	19.12.2024

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
- **BYOD:** Bring Your Own Device
- **KPIs:** Key Performance Indicators – Metrics used to measure the effectiveness and success of cybersecurity policies and standards.
- **Workstations:** Computers and related equipment used by employees for official tasks.
- **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.
- **Encryption:** The process of converting data into a secure format to prevent unauthorized access.
- **Firewall:** A security system that monitors and controls incoming and outgoing network traffic.
- **ECC-**1:2018: Essential Cybersecurity Controls
- **OTCC-**1:2022:Operational Technology Cybersecurity Controls

2 PURPOSE

This policy aims to define the requirements related to acceptable use in MCS in order to minimize the cybersecurity risks resulting from internal and external threats 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 applies to 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- Cybersecurity requirements must be followed in the policies, standards, and procedures approved by MCS.
2- Data and assets (hardware, information, or software) must be protected and handled as per their sensitivity and classification in accordance with the Data Protection Policy approved by MCS. Also, data confidentiality, integrity and availability must be ensured.
3- No printed matters should be left unattended on the shared printer.
4- External storage media must be kept in a secure and appropriate manner, such as ensuring that the temperature is set at a certain degree and stored in an insulated and safe place.
5- It is prohibited to disclose any of the MCS information, including systems and networks related information, to any unauthorized entity or party, whether internal or external.
6- It is prohibited to publish information about the MCS via the media and social media networks without permission of the Authorizing Official.
7- It is prohibited to use the MCS systems and assets to achieve personal benefit and business, or for any purpose not related to the activity and works of MCS.
8- It is prohibited to connect personal devices to networks and systems of MCS without prior authorization from the Cybersecurity Department. This should be done in accordance with Workstations, Mobile Devices and BYOD Security Policy approved by MCS.
9- It is prohibited to perform any activities intended to bypass the MCS protection systems, including anti-virus programs, firewall, and malware without prior authorization, and in accordance with the procedures approved by MCS.
10- The Cybersecurity Department retains its right to monitor and periodically review work-related systems, networks and personal devices, in order to monitor compliance with cybersecurity policies and standards approved by MCS.
11- The identification card of employee or visitors must visible in all facilities of MCS.
12- The Cybersecurity Department must be notified in case of loss, theft or leakage of MCS information.

13- Information and Asset Acceptable Use rules related to Information Processing systems must be followed up.
14- All MCS employees and staff must return all files, documents, information and assets in their possession upon work completion or expiry of their contract/agreement.
15- It is prohibited to transfer assets off-site without prior permission from relevant departments.
16- Assets that are off-site must be protected taking into account the various risks of working outside MCS buildings.
17- Sessions, meetings and contents related to security awareness campaigns organized by the MCS must be attended and should be abided by.
18- All staff must sign a statement of consent on Asset Acceptable Use approved by MCS.
19- All staff must approve and acknowledge the Code of Conduct and Acceptable Use Policy upon any review or update thereof.
20- Access to MCS assets must be according to roles and responsibilities required to perform tasks only.
21- Technical asset administrators must be alerted about cybersecurity patches to be implemented according to MCS Patch Management Policy.
22- Asset owners must review user access rights at defined and regular intervals.
23- The Cybersecurity Department must be notified when suspecting any activity that may harm MCS or its assets, such as suspected sites, cybersecurity risks or mail contents that may harm MCS.
24- In case of non-compliance with any item, MCS must explain and state the reasons.
25- Key performance indicators (KPIs) must be used to ensure correct and effective use of requirements and protect MCS information and technology assets.

4.2 Protection of Laptops

1- It is prohibited to use external storage media without prior authorization from Cybersecurity Department. When used, stored data must be encrypted according to MCS Encryption Standard.
2- Devices must be secured before leaving office by Sign out or Lock, whether leaving for a short time or after working hours.
3- It is prohibited to use or install hardware, tools, or applications unapproved by MCS on the laptop without prior authorization of IT Department.

4.3 Internet and Software Acceptable Use

1- Security messages that may arise while browsing the internet or internal networks must be treated cautiously and be dealt with only after contacting Cybersecurity Department.
2- It is prohibited to violate the rights of any person, or company protected by copyright, patent or other intellectual property, similar laws or regulations, including, but not

limited to, installation of unauthorized or illegal software for any business purposes, or use of external storage media without consent of MCS.

3- A secure and authorized browser must be used to access internal network or internet.
4- It is prohibited to use techniques that allow bypassing Proxy or Firewall to access Internet.
5- It is prohibited to upload or install Software and tools on MCS assets without prior authorization of Cybersecurity Department.
6- It is prohibited to use Internet for non-business purposes, including uploading media and files, as well as using file sharing software without prior authorization of Cybersecurity Department.
7- It is prohibited to conduct a security check to discover security vulnerabilities, including penetration testing, or monitoring MCS networks and systems, or third-party networks and systems without prior authorization of Cybersecurity Department.

4.4 Email Acceptable Use

1- It is prohibited to use email, telephone or e-fax for non-business purposes, noting that their use shall only be in accordance with cybersecurity policies and standards approved by MCS.
2- It is prohibited to exchange messages containing inappropriate or unacceptable content, including messages with internal and external parties.
3- Encryption techniques must be used when sending sensitive information via email or communication systems as per the MCS Data Protection Policy.
4- MCS email address should not be registered at any site not related to work.
5- MCS has the right to disclose emails' content after obtaining the necessary permits from the Representative and the Cybersecurity Department in accordance with the MCS's relevant approved procedures and regulations.
6- It is prohibited to open suspicious or unexpected emails and attachments, even if they appear to be from reliable sources.

4.5 Video Conferences and Web-based Communications

1- It is prohibited to use unauthorized tools or software to make calls or hold video conferences related to work.
2- It is prohibited to make calls or hold video conferences not related to work without prior authorization to use MCS's tools or software.
3- It is prohibited to hold meetings related to work in public places due to risk of leaking classified information.

4.6 Passwords Use

1- It is necessary to choose secure passwords and to safeguard MCS systems and assets passwords in accordance with MCS Identity and Access Management Policy. It is also necessary to choose passwords different from those of personal accounts, such as personal mail and social media accounts.
2- It is prohibited to share the password by any means, including electronic correspondence, voice calls, and paper writing. Users must not disclose passwords to any other party, including co-workers and employees of IT Department and immediately notify Cybersecurity Department immediately if this occurs.
3- Passwords must be changed on a regular basis according to Password Policy requirements or upon obtaining a new password from the system administrator.
4- It is prohibited to use previously used or common passwords. It is also prohibited to share user's password with anyone.

4.7 Office Use

1- It is necessary to abide by MCS's Secure and Clean Office Policy, and to make sure the desktop and screen are free of classified and sensitive information as per MCS's approved classifications.
2- It is prohibited to leave any MCS classified or sensitive information in places that are easily accessible, or accessed by unauthorized persons.
3- It is prohibited to leave office doors and cabinets containing classified and sensitive information open.

4.8 Cloud Computing

1- Data must be classified prior to being hosted with cloud computing and hosting service providers, and returned to the organization (in a usable format) upon service completion.
2- MCS environment (especially virtual servers) must be separated from other cloud computing environment of other organizations.
3- Location for hosting and storing MCS information must be inside the Kingdom and storing must be in accordance with the relevant legal and regulatory requirements.
4- Cybersecurity requirements for protection of cloud computing subscribers' data and information must be covered in accordance with the relevant legal and regulatory requirements, as a minimum:

5-1 Guarantees for ability to delete data safely upon expiry of relationship with service provider (Exit Strategy).

5-2 Use secure means to export and transfer data and virtual infrastructure.

5 ROLES AND RESPONSIBILITIES

1- **Policy Owner:** Cybersecurity Manager
2- **Policy Review and Update:** Cybersecurity Department
3- **Policy Implementation and Execution:** Human Resources 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- The 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 2-1-3 Asset Management