Malware Protection Policy

MCS Cybersecurity Department

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	Malware Protection Policy	19.12.2024

TABLE OF CONTENTS

1 ABBREVIATIONS & DEFINITIONS 4

2 PURPOSE 4

3 SCOPE 5

4 POLICY STATEMENTS 5

4.1 GENERAL REQUIREMENTS 5

4.2 MALWARE PROTECTION MECHANISMS AND TECHNIQUES CONFIGURATION 6

5 ROLES AND RESPONSIBILITIES 7

6 UPDATE AND REVIEW 7

7 COMPLIANCE 7

8 REFERENCES 7

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
- **KPI:** Key Performance Indicator, A measurable value used to evaluate the effectiveness of security measures
- **APTs (Advanced Persistent Threats):** Long-term cyberattacks that use sophisticated techniques, including zero-day malware.
- **Sandbox:** An isolated environment used to inspect and test suspicious content without affecting the main system.
- **Malware:** Malicious software designed to harm or exploit systems, including viruses, worms, and trojans.

2 PURPOSE

This policy aims to define the cybersecurity requirements related to the protection of MCS's information and technology assets against malware 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 MCS's information and technology assets (such as workstations, mobile devices, and servers) and applies to all personnel (employees and contractors) in the MCS.

4 POLICY STATEMENTS

4.1 General Requirements

1- MCS must provide appropriate, modern, reliable, and advanced protection mechanisms and techniques.

2- Protection mechanisms and techniques must be implemented and securely managed to protect workstations, mobile devices, servers, systems, and applications against malware.

3- Protection mechanisms and techniques must detect all types of malware (such as viruses, trojan horses, worms, spyware, adware, rootkits, and other types of malware).

4- Prior to selecting protection mechanisms and techniques, compatibility and secure integration with MCS's operating and information systems, such as Windows, UNIX, Linux, Mac, and others, must be ensured.

5- Protection solution updates must be tested in a separate environment, other than the operation and production environments, to ensure their safety before implementing them in the production environment.

6- Protection solutions must be capable to restore the definitions to a previous version if the update damages the systems or business requirements.

7- Access and identity procedures related to managing and operating protection solutions and their activities (e.g., disabling, modifying, etc.), must be implemented, limited to malware protection solution administrators, and reviewed periodically in accordance with the relevant approved policies in MCS.

8- Uninstalling, disabling, or reconfiguring protection solutions must be restricted and limited to protection solutions administrators only.

9- Cybersecurity Department must ensure the cybersecurity awareness of all personnel and educate them to handle malware and mitigate their risks.

10- Key Performance Indicators (KPI) must be used to ensure the continuous improvement and effective and efficient use of the protection requirements of workstations, servers, and third parties against malware.

4.2 Malware Protection mechanisms and techniques Configuration

1- Protection mechanisms and techniques configuration must be according to MCS's approved technical security standards taking into account the vendor's guidelines and recommendations.

2- Antivirus solutions must be configured on email servers to scan all inbound and outbound emails.

3- Antivirus solutions must be configured on email servers to restrict receiving or sending email attachments depending on file type and content.

4- Antivirus solutions must be regularly updated as per MCS's approved Patch Management Policy.

5- Updating is required for end-point devices to function.

6- Availability of protection solution servers must be guaranteed. Protection solutions must be compatible with the backup environment dedicated for non-critical functions and business.

7- Email messages must be filtered using modern protection solutions.

8- Access to websites and other online resources known to host malware must be prevented using a web content filtering solution.

9- All protection mechanisms and techniques must be synchronized centrally and with a reliable source.

10- Protection solutions must be configured to inspect suspicious content in separate environments, such as a sandbox.

11- Workstations and servers must be scanned periodically to ensure that they are malware-free.

12- Storage media must be scanned in a dedicated environment before their use if they are from outside MCS, or if they belong to MCS and are used on non-MCS systems, or by using the file and link scan feature on the National Portal for Cybersecurity Services "Haseen".

13- The use of external storage media in the production environment must be restricted unless secure mechanisms are developed and implemented for data transfer to the production environment.

14- The use of removable storage media must be restricted, and the required authorizations must be obtained before their use.

15- Physical and logical restriction, segmentation, and separation must be implemented when connecting MCS's systems and devices to external networks, such as the Internet, remote access, or wireless connection.

16- Protection solutions must be automatically updated upon the release of any vendors' new versions, subject to Patch Management Policy.

17- Protection solutions must be provided, implemented, and securely managed to protect email and Internet browsing against Advanced Persistent Threats (APTs) that usually use zero-day malware and viruses.
18- Protection solutions must be provided to detect and scan command execution.
19- Protection solutions must be provided to detect and scan new communication sessions.
20- Protection solutions must be configured to whitelist a specific list of application and program execution files to run on system servers and devices (including servers and end-points).
21- All workstations and servers must be protected with the end-point protection solutions approved by MCS.
22- Periodic reports on malware protection status and indicating the number and status of devices and servers running protection solutions (such as updated, outdated, or not connected, etc.) must be prepared and submitted to the Cybersecurity Manager.
23- Protection solutions must be centrally managed and constantly monitored.

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.

8 REFERENCES

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