Vulnerabilities Management 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	Vulnerabilities Management Policy	21.12.2024

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
- **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
- **Rollback Plan:** A contingency plan designed to revert systems to their previous state if a patch or change adversely affects system performance.
- **Haseen:** A platform for sharing cybersecurity threat information in Saudi Arabia, overseen by the National Cybersecurity Authority (NCA).

2 PURPOSE

This policy aims to define the cybersecurity requirements related to ensuring that technical vulnerabilities are detected in a timely manner and effectively remedied to prevent or reduce the exploitation of these vulnerabilities by cyberattacks, as well as mitigating their impact on MCS's business and protecting it from internal and external threats.

These requirements are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to ECC-1:2018, CSCC-1:2019 and other relevant legal and regulatory requirements.

3 SCOPE

This policy covers all MCS's information technology assets and applies to all personnel (employees and contractors) in the MCS.

4 POLICY STATEMENTS

4.1 General Requirements

1- Vulnerabilities must be scanned and assessed on a regular basis by a competent and qualified team to detect and assess technical vulnerabilities in a timely manner and remedy them effectively according to the relevant legal and regulatory requirements as follows:

Asset Type	Systems					
	All systems	Critical systems connected to the internet	Internal critical systems	Telework systems	Social media accounts systems	Cloud Computing Service Systems
	Frequency of vulnerability scanning and assessment					
Operating Systems	Monthly	Monthly	Monthly	Monthly	Monthly	Monthly
Databases	3 months	Monthly	3 months*	Monthly	Monthly	3 months
Network Devices	3 months	Monthly	3 months*	Monthly	Monthly	3 months
Applications	3 months	Monthly	3 months*	Monthly	Monthly	3 months

* The vulnerability scanning must be monthly, while the vulnerability assessment must be every three months.

2- Define systems, services, and technology components to be subject to vulnerability assessment as per the relevant legal and regulatory requirements.

3- Use reliable and approved methods and tools to detect vulnerabilities.

4- Assess vulnerabilities before publishing services or systems online, or upon any change to infrastructure or systems as per Cybersecurity in Information Technology Projects Policy approved by MCS.

5- Classify vulnerabilities as per risk level and remedied in line with the resulting cyber risks and MCS's Risk Management Methodology.

6- If a third party is assigned to conduct vulnerability assessment on behalf of MCS, third party cybersecurity requirements must be verified as per Third-party Cybersecurity Policy approved by the MCS and the relevant legal and regulatory requirements.

7- Communicate and subscribe with authorized and trusted cybersecurity resources “Threat intelligence", special interest groups and external subject matter experts to collect information about new threats and how to reduce potential vulnerabilities, in addition to participation with NCA via Haseen Platform. NCA approval is required upon subscription with other providers.

8- In case of MCS's subscription with other service providers to be informed of the latest vulnerabilities, the processes related to the receipt, analysis and remediation of vulnerabilities from internal and external sources must be developed.

9- Remedy all vulnerabilities as per their severity and classification according to the cybersecurity risk management framework adopted in MCS.

10- Develop a vulnerability management plan in MCS which will be overseen by an internal or external vulnerability assessment team.

11- Define a specific approach for effective remediation of vulnerabilities, prevention or mitigation of exploiting vulnerabilities, and reduction of impacts on business operation.

12- Maintain records of vulnerability assessments, updates and associated changes.

13- Develop procedures and standards for vulnerabilities assessment based on the work need.

14- Key performance indicators must be used to ensure the continuous improvement of vulnerabilities management requirements.

4.2 Vulnerabilities Remediation Requirements

1- Upon finalizing the vulnerability assessment, a report must be prepared to illustrate detected vulnerabilities, classification, and recommended remediation.

2- After vulnerability assessment report is sent and vulnerabilities are remedied by stakeholders, a vulnerabilities assessment must be conducted again to ensure remediation.

3- Patches from reliable and secure sources must be used as per Patch Management Policy.

4- Newly detected critical Vulnerabilities must be fixed as per ‘s Change Management Procedures approved by MCS.

5- Vulnerabilities reported by the cloud computing service provider must be managed and remedied.

6- A Rollback Plan must be developed and implemented if patches adversely affect performance of systems, applications, or services.

7- If vulnerabilities are not remedied or fixed for any reason, other controls must be implemented such as disabling the compromised service, or providing compensating controls such as firewall access control and similar solutions, monitor vulnerabilities for actual attacks and report such vulnerabilities and exploits to incident response team.

5 ROLES AND RESPONSIBILITIES

1- **Policy Owner:** Cybersecurity Manager
2- **Policy Review and Update:** Cybersecurity Department
3- **Policy Implementation and Execution:** IT 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 at 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 2-10-1 Vulnerabilities Management