Cybersecurity Management		
Penetration Testing Policy		
Doc: MCS-CS-POL-23	Issue/Rev: 1.0	Date: 21.12.2024

Penetration Testing Policy

MCS Cybersecurity Department

Cybersecurity Management		
Penetration Testing Policy		
Doc: MCS-CS-POL-23	Issue/Rev: 1.0	Date: 21.12.2024

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	Penetration Testing Policy	21.12.2024

Cybersecurity Management		
Penetration Testing Policy		
Doc: MCS-CS-POL-23	Issue/Rev: 1.0	Date: 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
- **Operational Technology / Industrial Control Systems:** Technology systems used to monitor and control physical devices and processes in industries like manufacturing.
- **Key Performance Indicator:** A measurable value that demonstrates how effectively an organization is achieving a business objective.
- **Industrial Control Systems:** Systems used to monitor and control industrial processes like manufacturing or energy distribution.

2 PURPOSE

This policy aims to define the cybersecurity requirements related to assessing and testing the effectiveness of MCS's defense, by simulating real attacks techniques and technologies, to discover unknown security weaknesses that might compromise MCS.

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

3 SCOPE

This Policy covers all systems and its technology components as well as all externally provided services (via internet) and its technology components including: infrastructure, websites, web applications, smart phones and tablets applications, emails, and remote access in MCS and applies to all personnel (employees and contractors) in MCS.

4 POLICY STATEMENTS

4.1 General Requirements

1- Rules of engagement document must be developed prior to the Penetration Testing process, which must cover the scope of testing, privileges, duration, target systems, testing mechanism, general conditions and requirements, etc.
2- The scope of penetration testing must include all technology components including: infrastructure, websites, web applications, smart phones and tablets applications, emails, and remote access, OT/ICS network environment in accordance with the relevant legal and regulatory requirements.
3- Penetration Testing must be conducted to evaluate and test the efficiency of cybersecurity capabilities regularly.
4- Penetration testing must be conducted on critical systems, their technology components and all their internal and external services at least every six months.
5- Penetration testing must be conducted on telework systems and all externally provided services (through the internet) and their technology components at least once a year.
6- Ensure that the testing effect is limited on the production environment (operating environment) or conduct penetration testing in a identical separate environment.
7- Passive testing must be conducted to review and examine systems, applications, networks, policies and procedures, and detect security vulnerabilities.
8- A plan for penetration testing that covers scope of work, start date, end date, methodology, and real-world attack scenarios must be developed and approved.
9- Ensure that the penetration testing does not impact systems and provided services in MCS .
10- A qualified team with relevant certificates and experience must be appointed to ensure effective penetration testing .
11- Penetration testing team must coordinate with stakeholders from MCS to follow the approved procedures and penetration testing plans, conduct the necessary analysis in order to define the false positive indicators, classify vulnerabilities and determine their causes.
12- Penetration testing data must be processed in a secure manner and must be collected, stored, transferred, and removed when it becomes unnecessary according to MCS Data and Information Protection Policy.

13- Penetration testing must be conducted to discover vulnerabilities of all forms, including vulnerabilities that usually result from application development errors without taking into account the Secure Code Development and Misconfigurations standard as well as the Exploitability of Identified Vulnerability.
14- If a third party is assigned to conduct penetration testing on behalf of MCS, third party cybersecurity requirements must be verified as per MCS's Third-party Cybersecurity Policy.
15- A report must be developed stating the testing results, recommendations must be made after completion of penetration testing process.
16- Penetration testing results must be classified based on their sensitivity, and remediated according to their cyber risks as per MCS risk management methodology
17- An action plan must be developed to remediate penetration testing results and illustrate risk impacts, treatment mechanism, implementation owner, duration and monitoring.
18- User accounts used to conduct penetration testing must be managed and monitored to ensure that they are only used for legitimate purposes and removed after testing.
19- Procedures and standards for penetration testing must be developed based on business need.
20- Key performance indicators must be used to ensure the continuous improvement and effective and efficient use of Penetration Testing requirements.

5 ROLES AND RESPONSIBILITIES

1- **Policy Owner:** Cybersecurity Manager
2- **Policy Review and Update:** Cybersecurity Department
3- **Policy Implementation and Execution:** Information Technology 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 2-11-1 Penetration Testing