



| | | | |
|------------------------------------|----------------|------------------|---|
| Cybersecurity Management | | |  الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company |
| Configuration and Hardening Policy | | | |
| Doc: MCS-CS-POL-06 | Issue/Rev: 1.0 | Date: 20.12.2024 | |

Configuration and Hardening Policy

MCS Cybersecurity Department

| | | | |
|------------------------------------|----------------|------------------|---|
| Cybersecurity Management | | |  الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company |
| Configuration and Hardening Policy | | | |
| Doc: MCS-CS-POL-06 | 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 | Configuration and Hardening Policy | 20.12.2024 |
| | | |
| | | |


| | | | |
|------------------------------------|----------------|------------------|---|
| Cybersecurity Management | | |  الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company |
| Configuration and Hardening Policy | | | |
| Doc: MCS-CS-POL-06 | Issue/Rev: 1.0 | Date: 20.12.2024 | |

TABLE OF CONTENTS

| | | |
|----------|---|----------|
| 1 | ABBREVIATIONS & DEFINITIONS | 4 |
| 2 | PURPOSE | 5 |
| 3 | SCOPE..... | 5 |
| 4 | POLICY STATEMENTS | 5 |
| 4.1 | GENERAL REQUIREMENTS | 5 |
| 4.2 | TECHNICAL SECURITY STANDARD DEVELOPMENT..... | 5 |
| 4.3 | CONFIGURATION AND HARDENING REVIEW AND IMPLEMENTATION | 6 |
| 5 | ROLES AND RESPONSIBILITIES..... | 7 |
| 6 | UPDATE AND REVIEW | 7 |
| 7 | COMPLIANCE | 7 |
| 8 | REFERENCES | 7 |

| | | | |
|------------------------------------|----------------|------------------|--|
| Cybersecurity Management | | | <div><div>MCSO</div><div>الشركة الكيميائية الحديثة للخدمات</div><div>Modern Chemicals & Services Company</div></div> |
| Configuration and Hardening Policy | | | |
| Doc: MCS-CS-POL-06 | Issue/Rev: 1.0 | Date: 20.12.2024 | |

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
- **KPI:** Key Performance Indicator - A measurable value that indicates how effectively an individual, team, or organization is achieving key business objectives.
- **CIS:** Center for Internet Security - A non-profit organization that develops best practices for securing IT systems and data.
- **SANS:** SysAdmin, Audit, Network, Security Institute - A cybersecurity training and certification organization that provides security research and education.
- **NIST:** National Institute of Standards and Technology - A U.S. government agency that develops security frameworks and guidelines for IT and cybersecurity.
- **SCAP:** Security Content Automation Protocol - A framework that automates security assessments and compliance checks using standardized security data.
- **SASO:** Saudi Standards, Metrology and Quality Organization - The regulatory body in Saudi Arabia that defines quality and measurement standards.
- **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.
- **Cybersecurity Logs:** Records of events related to network and system security, which help in detecting and analyzing potential threats.
- **Clock Synchronization:** The process of ensuring that all systems in a network use the same accurate time source, which is crucial for security and forensic analysis.
- **Configuration Hardening:** The practice of securing systems and applications by reducing vulnerabilities, disabling unnecessary services, and applying security settings.

| | | | |
|------------------------------------|----------------|------------------|---|
| Cybersecurity Management | | | <div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div> |
| Configuration and Hardening Policy | | | |
| Doc: MCS-CS-POL-06 | Issue/Rev: 1.0 | Date: 20.12.2024 | |

- ECC-1:2018: Essential Cybersecurity Controls
- OTCC-1:2022: Operational Technology Cybersecurity Controls

2 PURPOSE

This policy aims to define the cybersecurity requirements related to the protection, hardening, and configuration of MCS's information and technology assets 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 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- All information and technology assets and all approved applications and software used in MCS must be defined and documented.
- 2- MCS's workstations, systems, applications, network devices, servers, and security devices must be configured and hardened according to the technical security standards approved by the vendors, and as per the relevant legal and regulatory requirements and international best practices to prevent cyberattacks.
- 3- Print screen or screen capture features must be disabled for devices that create or process information based on the information classification.
- 4- Key Performance Indicators (KPIs) must be used to ensure the continuous improvement and effective and efficient use of configuration and hardening security protection requirements.

4.2 Technical Security Standard Development


- 1- The vendors' security configuration guidance must be used according to MCS's regulatory procedures and policies, the relevant legal and regulatory requirements, and international best practices.
- 2- Security configuration guidance must be used from trusted sources that are aligned with factory standards such as the Center for Internet Security (CIS), the SysAdmin, Audit, Network, Security (SANS) Institute, and the National Institute of Standards and Technology (NIST).

| | | | |
|------------------------------------|----------------|------------------|---|
| Cybersecurity Management | | | <div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div> |
| Configuration and Hardening Policy | | | |
| Doc: MCS-CS-POL-06 | Issue/Rev: 1.0 | Date: 20.12.2024 | |

- 3- MCS's technical security standards must be developed in line with the nature of business, the vendors' security configuration guidance, factory standards, and the relevant legal and regulatory requirements.
- 4- Technical security standards for all MCS's authorized information and technology assets, applications, and programs must be developed, documented, approved, and reviewed in line with international practices, MCS's approved regulatory procedures and policies, and the relevant legal and regulatory requirements.

4.3 Configuration and Hardening Review and Implementation

- 1- Configuration and hardening of all information and technology assets and applications must be reviewed at least once a year or in case any changes happen, and their implementation must be ensured according to cybersecurity guidelines, best practices, and vendors' recommendations, and in line with MCS's change management mechanisms.
- 2- Configuration and hardening must be reviewed before launching applications, technology projects, and changes related to information and technology assets.
- 3- Default configurations of all information and technology assets for remote work systems must be reviewed, and to ensure that fixed passwords and default backgrounds do not exist.
- 4- Enabling remote work features and services must be restricted on an as-needed basis, and potential cybersecurity risks must be assessed in case of a need to enable them, in line with the relevant legal and regulatory requirements.
- 5- An image of the MCS's configuration and hardening for information and technology assets must be approved and stored in a secure place as per the approved technical security standards.
- 6- An approved image must be used to install or update information and technology assets.
- 7- The necessary technologies must be provided to centrally manage configuration and hardening and ensure automatic implementation or/and update of configuration and hardening for all information and technology assets at pre-determined times, after conducting the required testing.
- 8- A Security Content Automation Protocol (SCAP) compliant configuration monitoring system must be implemented to verify that the configurations are in line with the approved technical security standards and are fully implemented. Any unauthorized changes must be reported.
- 9- Clock synchronization must be implemented centrally from an accurate and reliable source (such as relevant sources provided by Saudi Standards, Metrology and Quality Organization (SASO)).

| | | | |
|------------------------------------|----------------|------------------|---|
| Cybersecurity Management | | |  الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company |
| Configuration and Hardening Policy | | | |
| Doc: MCS-CS-POL-06 | Issue/Rev: 1.0 | Date: 20.12.2024 | |

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 2-3-1 Information System and Information Processing Facilities Protection