Cybersecurity Policy for Operational Technology

MCS Cybersecurity Department

DOCUMENT VALIDATION & DISTRIBUTION

<table>
<tr><th colspan="2">Prepared By:</th><th colspan="2">Reviewed By</th><th>Approved By</th></tr>
<tr><td colspan="2">Mubashar Rehman
NII Consultant

Fatmah Mahdi Ahmed
Cybersecurity Manager</td><td colspan="2"></td><td></td></tr>
<tr><th colspan="5">Distributed to:</th></tr>
<tr><td colspan="3">✓ All Department Manager
✓ General Manager</td><td colspan="2">✓</td></tr>
</table>

REVISION HISTORY

Issue /Rev	Revision Description	Date
1.0	Cybersecurity Policy for Operational Technology	22.12.2024

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 (OT):** Hardware and software systems used to monitor and control physical devices, processes, and events in an industrial setting.
- **Industrial Control Systems (ICS): Systems** used in industrial environments to control and automate processes, often involving devices like PLCs (Programmable Logic Controllers) and SCADA (Supervisory Control and Data Acquisition).
- **Demilitarized Zone (DMZ):** A network segment that is isolated from other network zones to increase security by limiting external access to internal systems.
- **Multi-Factor Authentication (MFA):** A security mechanism that requires users to present two or more separate forms of identification to access a system or network.
- **Safety Instrumented Systems (SIS):** Systems designed to monitor and control safety-critical processes, ensuring they operate within defined safety parameters to prevent hazardous incidents.
- **User Behavior Analytics (UBA):** A cybersecurity approach that involves analyzing user activities across systems to detect unusual or potentially malicious actions.
- **Critical National Infrastructure (CNI):** The physical and virtual assets essential for the functioning of a society and economy, such as energy, transportation, and communication systems.

- **Key Performance Indicator (KPI):** A measurable value that indicates the effectiveness of a cybersecurity program or process.
- **SCyWF:** Saudi Cybersecurity Workforce Framework-A national framework providing guidelines for the development of cybersecurity professionals in Saudi Arabia
- **Data Leakage Prevention (DLP):** Technologies and practices used to monitor and control the movement of sensitive data, preventing it from being accessed or transferred without proper authorization.
- **TTPs:** Tactics, Techniques, and Procedures, referring to the behaviors and methods used by cyber attackers
- **RTO:** Recovery Time Objective, the maximum acceptable time that an application can be down after a disruption
- **RPO:** Recovery Point Objective, the maximum acceptable amount of data loss measured in time before a disruption occurs

2 PURPOSE

This policy aims to define the cybersecurity requirements related to the MCS's operational technology, including industrial control systems and devices 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 (industrial control devices and systems and operating systems and its components) in MCS and applies to all personnel (employees and contractors) in MCS.

4 POLICY STATEMENTS

4.1 General Requirements

1- All approved MCS ‘s cybersecurity policies and requirements must be applied to MCS’s operational technology and industrial control systems (OT/ICS).

2- Zones within the ICS environment must be logically or physically segmented according to the zone's appropriate level, and data flow must be isolated between zones so that they are connected through specific choke points.

3- Strict restrictions and physical and logical segmentation must be implemented when connecting ICS networks to the internal network of the corporate zone and other networks in MCS, and access to business critical services on ICS networks from the internal network must be denied and restricted to authorized services.

4- Strict restrictions and physical and logical segmentation must be implemented when connecting ICS and industrial control networks to external networks by using security control system such as the demilitarized zone (DMZ).

5- Remote direct access to ICS networks must be prevented, and all connections must be routed to the jump hosts dedicated to such operations, secure, reinforced in the DMZ, and used only when needed while ensuring that Multi-Factor Authentication (MFA) principle and session recording are applied for a specified period of time.

6- Safety Instrumented Systems (SISs) must be isolated either logically or physically from other ICS networks.

7- Cybersecurity event logs must be activated on the OT/ICS network environment and related connections, and regularly monitored.

8- Cybersecurity event logs and audit trails must be activated for all OT/ICS assets.

9- Failed attempts to access the MCS’s monitoring systems must be detected and logged.

10- Continuous, in-depth cybersecurity log review and monitoring, covering all logs and audit trails must be conducted for all OT/ICS assets.

11- Monitoring, detecting, and analyzing User Behaviors Analytics (UBA) must be performed.

12- Upload or download activities of OT/ICS assets including Safety Instrumented Systems (SIS) must be detected.

13- All remote access sessions must be monitored.

14- Malicious events must be detected and analyzed.

15- Logging and monitoring of new alerts when new or unauthorized devices are connected to the OT/ICS networks must be performed.

16- OT/ICS Threat Intelligence must be used and incorporated to regularly tune and refresh alerts of Security Information.

17- All access control points between the network security boundaries and external connections must be monitored.

18- The OT/ICS security configuration must undergo periodic review.

19- Technical Security Standards for OT/ ICS must be defined, approved, and applied, taking into account the preferences of the manufacturers and developers of these systems in accordance with the Secure Configuration and Hardening Policy adopted in MCS.

20- OT/ICS Vulnerability Management must be performed periodically, and vulnerabilities must be addressed based on their classification and their cybersecurity threats and in line with MCS's Vulnerability Management Policy.

21- Scope and activities of vulnerability assessments must be defined for OT/ICS environment as part of MCS’s formal vulnerability management while ensuring limited or no impact on the production environment.

22- Remediation of newly discovered critical vulnerabilities presenting significant risks to the OT/ICS environment must be performed in a timely manner.

23- The cybersecurity requirements for vulnerability management in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.

24- OT/ICS Patch Management must be implemented periodically as per MCS Patch Management Policy.

25- The automatic and default configuration of these systems must be reviewed to make sure that their settings do not facilitate third-party access or pre-defined access or pass rights.

26- Access to OT/ICS locations within MCS must be restricted to authorized personnel only, as per the MCS's Identity and Access Management and Physical Security Policy and in line with their operational requirements.

27- Backup Recovery must be periodically tested, and Backup and Recovery Management cybersecurity requirements must be implemented as per MCS Backup and Recovery Management Policy.

28- OT/ICS related CNI data and information must be identified, classified, protected, and handled based on their classification as per the MCS relevant legislations and laws.

29- Electronic and physical data (at rest and in transit) must be protected at a level consistent with its classification.

30- Data Leakage Prevention (DLP) mechanisms must be used to protect the classified data and information.

31- Secure wiping mechanisms for configuration details and stored data from OT/ICS assets prior to decommissioning must be implemented.

32- Transfer or usage of OT systems' data in any environment other than production environment must be limited, except after applying strict controls for protecting that data.

33- Cybersecurity awareness must be provided to MCS's personnel along with the required cybersecurity training, skills, and capabilities.

34- MCS must develop and accurate and up-to-date inventory of their OT/ICS assets.

35- Automated solution to collect asset inventory information must be utilized.

36- OT/ICS asset inventory records must be stored securely.

37- Asset owners for OT/ICS assets must be identified and involved throughout the relevant asset inventory management lifecycle.

38- Criticality rating for all assets must be assigned, documented, and approved by asset owners.

39- Clear roles and responsibilities must be defined and assigned to all stakeholders involved in the application of OT/ICS cybersecurity controls at MCS.

40- Cybersecurity requirements must be included in MCS's project management methodology and procedures to protect the confidentiality, integrity, and availability of the operational and technical works of ICS in accordance with the general cybersecurity policy adopted by MCS and relevant legal and regulatory requirements.

41- Cybersecurity levels must not be affected by the application of change requests in the environment containing ICS after analyzing and controlling vulnerabilities.

42- MCS must conduct OT/ICS security awareness campaigns.

43- Customized training, qualifications, knowledge, and professional skillsets must be provided to all personnel with access to the OT/ICS assets. The MCS is encouraged to utilize the reference material provided in the Saudi Cybersecurity Workforce Framework (SCyWF).

44- Participation in OT/ICS authorized and/or specialized organizations and groups must be encouraged.

45- OT/ ICS procedures and standards must be developed and approved based on business needs.

46- Key performance indicators (KPI) must be used to ensure the continuous improvement and effective and efficient use of cybersecurity requirements related to the protection of industrial control systems and devices.

4.2 OT Protection

1- Advanced and up-to-date antivirus and malware protection solutions for ICS must be implemented and configured according to the related malware protection policy and standards at MCS.

2- ICS networks systems and devices (e.g., proxy servers, firewalls, and data diodes) must be configured to block or restrict unauthorized traffic.

3- MCS's external storage media and mobile devices (including laptops, mobile configuration devices, network test devices) must not be connected to OT/ICS or their technology components without MCS's prior permission and after considering potential risks.

4- OT/ICS data confidentiality, integrity, and availability must be ensured in accordance with MCS data protection policy, and related legal and regulatory requirements.

5- Encryption must be used to protect data and information assets in accordance with the encryption policy adopted at MCS and related legal and regulatory requirements.

6- The multi-tier architecture principle must be adopted for OT/ICS web applications.

7- Threat Intelligence must be used to identify technologies and procedures (TTPs) used by Activity Groups targeting OT/ICS.

8- Cybersecurity risks to OT/ICS must be assessed periodically in accordance with the MCS cybersecurity risk management policy and other related legislations. Such assessments must include the assessment of third-party cybersecurity risks, including OT/ICS manufacturers, and suppliers of ICS products and services.

9- Cybersecurity risks and their OT/ICS requirements related to MCS's workers must be effectively addressed before, during and upon the termination of their employment, as per the organizational policies or procedures by MCS and the relevant legal and regulatory requirements.

10- Screening/vetting of all personnel (including employees and contractors) who have access or can utilize OT/ICS assets must be conducted prior to granting them access.

4.3 Cybersecurity Incident and Threat Management and Disaster Recovery

1- Assessment and evaluation of the efficiency of cybersecurity enhancement capabilities for OT/ICS assets at MCS must be conducted through penetration tests.

2- Scope and activities of penetration testing must be defined to ensure the coverage of OT/ICS environment and networks connected to the operational network by qualified team.

3- Penetration testing must only be conducted with limited or no impact on the production environment, or on an identical separate environment.

4- Penetration testing for OT/ICS systems must be conducted periodically.

5- Alternative testing methods (such as passive testing mechanisms) must be defined and implemented to collect relevant information when a potential impact to operational production environment may occur.

6- Redundancy must be implemented to critical networks, media, and devices in the OT/ICS assets in accordance with the periodic cybersecurity risk assessment.

7- OT/ICS cybersecurity resilience requirements must be included in the Business Continuity Plan (BCP), including the Business Impact Analysis (BIA), Recovery Time Objective (RTO), and Recovery Point Objective (RPO).

8- OT/ICS cybersecurity resilience requirements must be included in the Disaster Recovery Plan (DRP).

9- A contingency plan must be developed and approved to maintain or restore business operations from known valid backups in the event of cybersecurity incidents and ensure business continuity.

10- OT/ICS cybersecurity incident response plans and escalation plans must be defined as per MCS's Cybersecurity Incident and Threat Management Policy and other related legislations, and virtual plan exercises must be conducted periodically.

11- Cybersecurity incident response plans must be integrated and aligned with organizational plans and its procedures.

12- Formal incident response and root cause analysis for any detected cybersecurity incidents must be conducted.

13- Sequence of incident response activities necessary to restore normal operations must be defined.

14- Incident communications plan must be established.

15- OT/ICS including Safety Instrumented Systems (SIS) recovery procedures must be included in the incident response, system recovery plans, and business continuity plans of MCS.

16- Trainings and skillsets for the organization's personnel (including employees and contractors) to respond to OT/ICS cybersecurity incidents must be provided.
17- Cybersecurity incident response capabilities, readiness, and plan must be periodically tested by performing cyber-attack simulations exercises.
18- Threat Intelligence information must be used to identify Tactics, Techniques, and Procedures (TTPs) of activity groups targeting OT/ICS systems.
19- OT/ICS cybersecurity incident response plans must be aligned with the approved IT incident response plans, crisis management plans, and business continuity plans at MCS.
20- Activities required to maintain a minimum level of OT/ICS operations must be identified, and systems must be able to operate at an acceptable level of security when an error occurs due to a cybersecurity incident.
21- Incident analysis and Root Cause Analysis of cybersecurity incidents must be conducted systematically after incident detection.
22- Incident Communications Plan must be developed when cybersecurity incidents occur.
23- Owners and response teams must be aware of OT/ICS cybersecurity incident response plans by providing the organization employees with the required skills and training courses.
24- A disaster recovery plan for OT/ICS must be documented and include the following:
    - Develop the required response to events of varying durations and severity levels that would activate or deactivate the recovery plan.
    - Determine the sequence of the cybersecurity incident response activities required to restore normal operations.
    - Determine the procedures for restarting OT/ICS or operating them in manual mode.
    - Define the roles and responsibilities of responders and personnel authorized for physical and cyber access to the ICS.
    - Review processes and procedures for information asset backups and secure storage.
    - Define complete and up-to-date logical network diagram and current configuration information for all ICS technology components.
25- Cybersecurity incident response capabilities, readiness level, and approved plan must be tested periodically through Attack Simulation Exercises.

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