Third-Party Cybersecurity 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	Third-Party Cybersecurity 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
- **Outsourcing:** The practice of obtaining services or products from an external supplier rather than using internal resources.
- **Key Performance Indicators (KPIs):** Metrics used to evaluate and ensure the efficiency and continuous improvement of third-party cybersecurity measures.
- **Non-Disclosure Agreement (NDA):** A legal contract that ensures third-party personnel maintain confidentiality regarding sensitive information during and after employment or collaboration.
- **National Data Management Office (NDMO):** A governing body responsible for regulating data management practices and ensuring compliance with national data protection standards.

2 PURPOSE

This policy aims to define the cybersecurity requirements related to the protection of MCS's information and technology assets against cybersecurity risks related to third parties, including information technology outsourcing and managed services.

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 and all the services provided to MCS by third parties and their personnel, including information technology outsourcing and managed services, and it applies to all personnel (employees and contractors) in MCS.

4 POLICY STATEMENTS

4.1 General Requirements

1- Procedures must be documented, approved, and applied to manage MCS's relation with third parties before, during, and after the end of the contractual relationship.

2- A cybersecurity risk assessment on third parties and provided services must be conducted, including but not limited to, reviewing third-party projects in MCS, periodically reviewing the cybersecurity event logs of third-party services (if possible) before and during the relation as per MCS's approved Cybersecurity Risk Management Policy, and identifying the required protection controls that should be applied for the effective management of the detected cybersecurity risks.

3- Outsourcing and managed service companies that provide services to support or operate critical systems must undergo a vetting or screening process.

4- Contracts and agreements with third parties must include MCS's cybersecurity requirements, as well as clauses binding the third parties to comply with MCS's cybersecurity policies and other relevant legal and regulatory requirements.

5- Third-party personnel' contracts must include cybersecurity responsibilities and clauses of Non-Disclosure and secure deletion of MCS's data (during and after the end or termination of the employment relationship with MCS).

6- It must be ensured that third parties manage their cybersecurity risks.

7- Third parties must grant MCS the necessary permissions to conduct tests to verify the third parties' compliance with MCS's cybersecurity requirements and provide the required reports when needed.

8- Key Performance Indicators (KPIs) must be used to ensure the continuous improvement and efficient and efficient application of third-party cybersecurity requirements.

4.2 Cybersecurity Requirements for Information Technology Outsourcing and Managed Services Provided by Third Parties

Third parties must be carefully selected for information technology outsourcing and managed services, and the following, as a minimum, must be verified:

1- A cybersecurity risk assessment must be conducted, and effective controls on risks must be ensured before signing contracts and agreements with third parties or if changes occur in relevant legal and regulatory requirements.

2- Cybersecurity managed service centers for operation and monitoring that use remote access must be completely present inside the Kingdom of Saudi Arabia.

3- Outsourcing services for critical systems must be provided by national companies and entities as per the relevant legal and regulatory requirements.

4- Outsourcing and managed services that deal with classified data must be provided by national companies and entities as per the relevant legal and regulatory requirements.

4.3 Cybersecurity Requirements for Third Party Personnel

1- Outsourcing and managed service companies and their personnel working on critical systems and having classified data access must undergo screening or vetting.

2- Third-party personnel who are expected to have direct or indirect access to MCS's assets must sign an undertaking to protect information confidentiality before starting the work relation, as per the format approved by MCS.

3- Third-party personnel must be educated about MCS's cybersecurity requirements, and their compliance must be ensured.

4.4 Cybersecurity Requirements for Authentication and Access Controls

1- Third parties must develop approved procedures to grant and revoke access to all information and technology systems that process, transmit, or store MCS's information, in line with MCS's cybersecurity requirements and the objectives the cybersecurity controls.

2- Third-party personnel access to MCS's information must be restricted, and information must be processed securely, while ensuring continuous monitoring of access processes.

3- Password controls must be implemented for all users with access to MCS's information in line with MCS's cybersecurity requirements and the objectives the cybersecurity controls.

4- Access rights must be revoked upon the end/termination of the service of any third-party employee with access to MCS’s information or information and technology assets or in the event of a change in their job role that eliminates the need for continued access.

5- Third parties must review access rights regularly as per MCS's approved Identity and Access Management Policy.

6- Audit records must be securely stored, maintained, and made available at MCS's request and as per the relevant legal and regulatory requirements.

4.5 Change Management Cybersecurity Requirements

1- Third parties must follow a formal and appropriate change management process as per MCS's policies and procedures.
2- Changes to MCS's information and technology assets must be reviewed and tested before their implementation in the production environment.
3- Major changes planned or introduced to MCS's information and technology assets must be communicated to MCS's relevant stakeholders.

4.6 Cybersecurity Incident Management and Business Continuity Requirements

1- Third-party contracts and agreements must include requirements related to cybersecurity incident reporting and informing MCS of any cybersecurity incident that the third-party faces.
2- Communication procedures between third parties and MCS must be defined and documented, to be used in case of any cybersecurity incident that the third-party faces or to report vulnerabilities. These procedures must be reviewed and updated periodically.
3- An appropriate business continuity plan must be developed to avoid the unavailability of the services provided to MCS in line with MCS’s business continuity and disaster recovery plan requirements.

4.7 Data and Information Protection Requirements

1- MCS's information and data residing on all systems, and processed or stored by third parties, must be classified according to MCS's approved Data Classification Policy.
2- Third parties must process, store, and destruct MCS’s information and data according to MCS’s approved Data and Information Protection Policy and Standard.
3- Third-party contracts and agreements must include the ability to securely delete the MCS’s data at the third party’s side at the end or termination of the contractual relationship, with the provision of evidence of such deletion.
4- Third parties must apply appropriate encryption controls to protect information and data based on their classification at MCS and ensure their confidentiality, integrity, and availability in line with MCS's approved Cryptography Standard.
5- Third parties must regularly back up MCS's information and data as per MCS's Backup and Recovery Management Policy.
6- MCS’s information and data residing in critical systems and personal data processed by third parties must not be processed, stored, or used in the testing environment unless restrict controls are applied to protect such data, such as data masking, data scrambling, or data anonymization, and after obtaining the necessary approvals from the concerned departments in MCS to ensure data protection and privacy as per the guidelines and requirements of the National Data Management Office (NDMO).

7- MCS's information and data residing in critical systems and processed or stored by third parties must not be transmitted out of the production environment.

4.8 Audit

1- MCS must audit any related processes and systems whenever deemed necessary or appropriate.
2- Third-party personnel must be fully cooperative with MCS’s event log review and audit activities including implemented reviews.

5 ROLES AND RESPONSIBILITIES

1- **Policy Owner:** Cybersecurity Manager
2- **Policy Review and Update:** Cybersecurity Department
3- **Policy Implementation and Execution:** Cybersecurity Department, Information Technology Department, Human Resources Department, Legal Department, and Procurement 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 4-1-1 Third-Party Cybersecurity