Human Resources 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	Human Resources 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
- **KPI:** Key Performance Indicator: Metrics used to measure and ensure the effectiveness of cybersecurity policies and compliance.
- **Cloud Computing:** A technology that enables storage, processing, and access to data over the internet rather than on local computers.
- **Non-Disclosure Agreement (NDA):** A legal contract ensuring that employees do not disclose sensitive company information during or after their employment.
- **Need-to-Know Principle:** A security concept ensuring that employees only have access to the data necessary for their job functions.
- **Security Screening:** Background checks and security assessments conducted for personnel handling sensitive data or critical system functions.

2 PURPOSE

This policy aims to define the cybersecurity requirements related to personnel in MCS in order to minimize the cybersecurity risks resulting from internal and external threats 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 applies to all personnel (employees and contractors) in MCS.

4 POLICY STATEMENTS

4.1 General Requirements

1- Limit and approve cybersecurity requirements related to personnel before, during and at the end/termination of employment at the organization.

2- The MCS must conduct cybersecurity awareness campaigns for all personnel.

3- Review cybersecurity requirements related to Human Resources at least once a year including the controls related to the organization personnel on a regular basis. Any changes must be documented and approved by the organization representative then update this policy accordingly.

4- Fill critical systems related functions in the MCS with highly qualified Saudi nationals.

5- Define knowledge, skills and capabilities required for different cybersecurity functions accurately.

6- Fill cybersecurity functions with qualified Saudi nationals in cloud computing service provider's data centres within the Kingdom of Saudi Arabia.

7- Implement human resources cybersecurity controls throughout the employee's lifecycle in MCS, which includes the following phases:
   - Pre-employment
   - During service period
   - At the end or termination of employment

8- Implement cybersecurity requirements related to the personnel responsible for managing and maintaining social media accounts as per cybersecurity policies, procedures and processes of social media accounts.

9- Personnel of MCS must understand and agree on their job roles, cybersecurity requirements and responsibilities.

10- Ensure that cybersecurity risks related to personnel (employees and contractors) of cloud computing service providers and cloud computing service subscribers are effectively addressed before, during, and at the end/termination of employment, in accordance with the policies and regulatory procedures, and relevant legal and regulatory requirements.

11- Include responsibilities of cybersecurity and Non-Disclosure Agreement clauses in the contracts of MCS personnel (to be included during and after the end/termination of employment with MCS).

12- Include cybersecurity violations in the Human Resources violations regulation in MCS.

13- Personnel information must not be accessed without prior authorization.

14- Use Key Performance Indicator (KPI) to ensure continuous improvement and proper and effective use of cybersecurity requirements related to human resources.

4.2 Pre-employment

1- Personnel must undertake to comply with cybersecurity policies before being granted access to MCS systems.

2- Employee roles and responsibilities related to cybersecurity must be defined in job description, taking into account the application of non-conflict of interest's principle.

3- Cybersecurity roles and responsibilities must include the following:
- Protect all MCS assets from unauthorized access or vandalizing those assets.
- Implement all required cybersecurity related activities.
- Comply with MCS cybersecurity policies and standard.
- Adhere to the cybersecurity risk awareness program.

4- Approve and sign all cybersecurity policies by personnel as a prerequisite for accessing cloud-based technology systems.

5- Conduct security screening to personnel in cybersecurity functions, privileged access technology functions, and critical systems functions.

6- Conduct security screening to personnel with access to cloud computing services critical tasks such as key management, service management and access control.

4.3 During Employment

1- Offer an awareness program to all MCS personnel to increase the level of cybersecurity awareness periodically.

2- Provide cybersecurity awareness through all available channels used in the MCS including social media accounts of MCS.

3- The Human Resources Department must inform the relevant functions of any change in roles or responsibilities of personnel to take the necessary actions related to access cancellation or modification.

4- Ensure that all human resources cybersecurity requirements are applied.

5- Include the extent of cybersecurity compliance in employee assessment aspects.

6- Apply need-to-know principle in task assignment.

4.4 End or Termination of Employment

1- Define employment expiry or termination procedures in a manner covering cybersecurity requirements.
2- The Human Resources Department must inform the relevant units in case employment expiry or termination to take the necessary actions.
3- Ensure that all MCS assets are returned and personnel access rights are cancelled on their last working day and prior to obtaining the necessary clearance.
4- Define responsibilities and duties that will remain in effect after personnel end of employment in MCS, including the information confidentiality agreement, provided that such responsibilities and duties are included in all personnel contracts.

5 ROLES AND RESPONSIBILITIES

1- **Policy Owner:** Cybersecurity Manager
2- **Policy Review and Update:** Cybersecurity Department
3- **Policy Implementation and Execution:** Human Resources 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 1-9-1 Cybersecurity in Human Resources