



| | | | |
|--------------------------|----------------|------------------|---|
| Cybersecurity Management | | |  الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company |
| Email Security Policy | | | |
| Doc: MCS-CS-POL-17 | Issue/Rev: 1.0 | Date: 22.12.2024 | |

Email Security Policy

MCS Cybersecurity Department

| | | | |
|--------------------------|----------------|------------------|--|
| Cybersecurity Management | | | <div> الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div> |
| Email Security Policy | | | |
| Doc: MCS-CS-POL-17 | Issue/Rev: 1.0 | Date: 22.12.2024 | |

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 | Email Security Policy | 22.12.2024 |
| | | |
| | | |


| | | | |
|--------------------------|----------------|------------------|---|
| Cybersecurity Management | | |  الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company |
| Email Security Policy | | | |
| Doc: MCS-CS-POL-17 | Issue/Rev: 1.0 | Date: 22.12.2024 | |

TABLE OF CONTENTS

| | | |
|-----|-----------------------------------|---|
| 1 | ABBREVIATIONS & DEFINITIONS | 4 |
| 2 | PURPOSE | 5 |
| 3 | SCOPE..... | 5 |
| 4 | POLICY STATEMENTS | 5 |
| 4.1 | GENERAL REQUIREMENTS | 5 |
| 5 | ROLES AND RESPONSIBILITIES..... | 6 |
| 6 | UPDATE AND REVIEW | 7 |
| 7 | COMPLIANCE | 7 |
| 8 | REFERENCES | 7 |

| | | | |
|--------------------------|----------------|------------------|---|
| Cybersecurity Management | | | <div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div> |
| Email Security Policy | | | |
| Doc: MCS-CS-POL-17 | Issue/Rev: 1.0 | Date: 22.12.2024 | |

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
- **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, machinery, 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 cover the cybersecurity policy and procedures.
- **ECC-1:2018:** Essential Cybersecurity Controls
- **OTCC-1:2022:** Operational Technology Cybersecurity Controls
- **DLP:** Data Leakage Prevention, Technologies used to detect and prevent data from being leaked, either accidentally or maliciously, through channels like email
- **APT:** Advanced Persistent Threat, A prolonged and targeted cyberattack designed to gain unauthorized access to sensitive data
- **SPF:** Sender Policy Framework, an email authentication method used to prevent email spoofing by verifying the sending server's IP address
- **DKIM:** DomainKeys Identified Mail, an email authentication method that uses cryptographic authentication to verify the sender's identity and ensure the integrity of the email content
- **DMARC:** Domain-based Message Authentication, Reporting, and Conformance, An email validation system that helps prevent email spoofing by ensuring that SPF and DKIM are properly configured
- **MFA:** Multi-Factor Authentication, A security method that requires more than one verification factor to access email systems remotely or via webmail
- **Man-in-the-Middle Attack:** A cyberattack where the attacker secretly intercepts and potentially alters the communication between two parties

| | | | |
|--------------------------|----------------|------------------|---|
| Cybersecurity Management | | | <div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div> |
| Email Security Policy | | | |
| Doc: MCS-CS-POL-17 | Issue/Rev: 1.0 | Date: 22.12.2024 | |

- **KPIs:** Key Performance Indicators, Metrics used to measure and ensure the effectiveness of email protection and security measures
- **Email Gateway:** A server or software that filters and processes email traffic before it reaches the internal network to prevent harmful content such as spam or malware
- **Open Mail Relay:** A mail server that allows anyone on the internet to send email through it, often used in spam attacks and should be disabled for security purposes
- **Haseen:** National Portal for Cybersecurity Services in Saudi Arabia that provides email authentication services to prevent email fraud and improve security

2 PURPOSE

This policy aims to define the cybersecurity requirements related to the protection of MCS's email 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 MCS's information and technology assets (including email systems) and applies to all personnel (employees and contractors) in the MCS.

4 POLICY STATEMENTS

4.1 General Requirements

- 1- The necessary technologies to protect confidentiality, integrity, and availability of email messages during transmission and storage must be used and updated constantly.
- 2- Email protection, analysis, and filtering technologies must be used to block suspicious email messages, such as spam and phishing email messages.
- 3- The necessary technologies, such as Data Leakage Prevention (DLP), must be used to protect data against leakage via email from inside or outside MCS.
- 4- Technologies must be used to protect email servers against Advanced Persistent Threats (APTs) and zero-day malware.
- 5- Technologies must be used to inspect email message attachments and links in a sandbox before they reach the user's mailbox, whether such email messages are sent from inside or outside MCS.
- 6- Modern technologies must be used to ensure the reliability of MCS's incoming email message domains, including but not limited to, using the email authentication service within the National Portal for Cybersecurity Services (Haseen), and applying Send Protection Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based


| | | | |
|--------------------------|----------------|------------------|--|
| Cybersecurity Management | | | <div> الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div> |
| Email Security Policy | | | |
| Doc: MCS-CS-POL-17 | Issue/Rev: 1.0 | Date: 22.12.2024 | |

Message Authentication, Reporting and Conformance (DMARC) verification protocols to prevent email spoofing.

- 7- The necessary technologies to encrypt email messages containing classified information must be used in accordance with MCS's regulatory procedures and policies.
- 8- Multi-Factor Authentication (MFA) must be implemented for remote email access and webmail login.
- 9- Email messages must be archived and backed up periodically as per MCS's approved and related regulatory procedures and policies.
- 10- Generic accounts' owners and their responsibilities must be identified.
- 11- Secure access to email messages must be implemented and restricted to MCS's personnel only.
- 12- The necessary measures must be taken to prevent the use of MCS's email for non-authorized business purposes.
- 13- The System Administrator must not be allowed to access any personnel's information and email messages without prior authorization and must follow defined and approved procedures.
- 14- The size and type of inbound and outbound email attachments and the capacity of the mailbox must be determined for each user. Sending group messages to many users must be limited.
- 15- Email messages sent to outside MCS must be appended with a disclaimer.
- 16- Email messages must be classified according to the criticality of their attachments and information in accordance with MCS's approved Data and Information Classification Policy.
- 17- Open mail relay services must be disabled on the server.
- 18- The use of email must be prohibited for privileged accounts.
- 19- Connections between email gateways must be encrypted to prevent inactive man-in-the-middle attacks.
- 20- Cybersecurity Department must ensure the cybersecurity awareness of all personnel and educate them to handle secure email services and detect phishing emails.
- 21- Key Performance Indicators (KPIs) must be used to ensure the continuous improvement and efficient and effective use of email protection 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 and Cybersecurity Department
- 4- **Policy Compliance Measurement:** Cybersecurity Department

| | | | |
|--------------------------|----------------|------------------|--|
| Cybersecurity Management | | | <div> الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div> |
| Email Security Policy | | | |
| Doc: MCS-CS-POL-17 | Issue/Rev: 1.0 | Date: 22.12.2024 | |

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 2-4-1 Email Protection