Network Security 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	Network Security 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
- **Defence-in-Depth:** A multi-layered security strategy to protect networks.
- **Cybersecurity Event Logs:** Recorded logs of network and system activities for security monitoring.
- **Patch Management:** The process of updating and managing security patches on systems.
- **Firewall:** A network security system that monitors and controls incoming and outgoing traffic.
- **VLAN (Virtual Local Area Network**): A segmented network to separate critical systems from other networks.
- **Intrusion Prevention Systems (IPS):** Security technology to detect and prevent network threats.
- **HIDS/HIPS (Host Intrusion Detection/Prevention Systems): Security** tools to detect and prevent threats on individual devices.
- **APT (Advanced Persistent Threat):** A long-term cyberattack using sophisticated malware techniques.
- **DDoS (Distributed Denial of Service):** A cyberattack that overwhelms systems with excessive traffic.

- **Proxy:** A server that acts as an intermediary for internet access, filtering and analyzing traffic.
- **DNS Security:** Security mechanisms to protect against domain name system threats.
- **SSL/HTTPS Inspection:** The process of decrypting and analyzing encrypted web traffic.
- **VPN (Virtual Private Network):** A secure encrypted connection for remote network access.
- **Whitelisting:** A security practice allowing only pre-approved connections or applications.

2 PURPOSE

This policy aims to define the cybersecurity requirements related to MCS's networks and network devices, to minimize cybersecurity risks resulting from internal and external threats at MCS.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to ECC-1:2018 and CSCC-1:2019, in addition to other related cybersecurity legal and regulatory requirements.

3 SCOPE

This policy covers all networks and network devices in the MCS and applies to all personnel (employees and contractors) in MCS.

4 POLICY STATEMENTS

4.1 General Requirements

1- All network devices of MCS must be identified, kept up to date and approved.

2- Leading global technical security standard controls for all network devices used in MCS must be identified and applied and Defence-in-Depth principle on the network must be applied.

3- Access to MCS’s networks must be managed according to Identity and Access Management Policy where connection to network is available when needed and to authorized users only.

4- Logs for all devices and systems of MCS must be enabled , recorded and maintained , as per the organization's approved Cybersecurity Event Logs and Monitoring Management Policy.

5- Maintain and update network design documents must be on an ongoing basis.

6- Configure clock synchronization must be on all servers to synchronize time from a trusted source.

7- Implement the requirements of all policies related to network security adopted by MCS must including but not limited to , the following:

- Email security policy approved by MCS as per the relevant policies and legal and regulatory requirements.
- Patch Management Policy approved by MCS as per the relevant policies and legal and regulatory requirements.
- Web Application Security Policy approved by MCS as per the relevant policies and legal and regulatory requirements.

8- Key performance indicators must be used to ensure the continuous improvement and effective and efficient use of Cybersecurity Network Security requirements.

4.2 Network Protection

1- Develop and approve procedures must be used to grant and deny access to MCS networks , according to MCS's Identity and Access Management Policy.

2- Access to network must be granted based on a request submitted by user to the Information Technology Department indicating the type, duration and reasons of request.

3- In case of addition or amendment to firewall rules, necessary approvals must be obtained and network administrator must document the business requirements and request details in firewall system.

4- Username and password must be used to access MCS's network according to MCS approved Identity and Access Management Policy.

5- Provide technologies necessary must be used to restrict and manage access to network services, protocols and ports.

6- Restrict all physical data ports must be within MCS's facilities by port security or port-based authentication in order to reduce the exposure of network and possibly have unauthorized devices connect while being undetected.

7- Restrict and open network ports, protocols, and services must be used for remote access operations, especially on internal and critical systems as needed.

4.3 Third Parties Access Controls to the Network

1- Granting access to the MCS network to third parties must be subject to cybersecurity requirements mentioned in the third party's cybersecurity policy approved by MCS.

2- Secure encryption and authentication mechanisms must be used to transfer data to and from third parties.

3- A specified duration must be granted to third parties to access MCS's network as agreed with the system owner.

4- User and third parties access rights must be regularly reviewed according to MCS's cybersecurity policies.

5- Remote Access Management and Authentication (RAM) must be prevented on devices located in the organization's External-Facing Host.

6- Third-party personnel must be prevented from connecting to the network or WI-FI of MCS without vulnerabilities check in addition to updating the antivirus program, making the proper configuration and ensuring that their activities can be monitored.

4.4 Network Protection

1- Segment and segregate networks must be physically and logically using firewall and defence-in-depth mechanisms.
2- Segment critical systems network (VLAN) must be physically and logically.
3- Segregate production environment networks must be logically from testing environment network and other networks.
4- Monitor internal and external networks must be used for suspected activities.
5- Prevent connecting critical systems to the internet must be used if they are providing internal service to MCS and there is no need for remote access.
6- Segregate must be used for Voice Over IP "VOIP" network logically from data network.
7- Appropriate technologies must be used to secure browsing and internet connectivity through restricting use of suspicious websites., file storage/sharing and remote access websites.
8- Approve periodic update packages and security patches of assets in the production environment must be by the manufacturer and test them in a sandbox environment before being applied to the production environment.
9- Protection mechanisms must be securely implemented, managed and regularly updated to protect the internet browsing channel against Advanced Persistent Threats (APT) that contains usually viruses and zero-day malware .
10- Prevent connecting internal network directly to the internet. Connection must be via proxy to analyse and filter data from and to MCS .
11- Firewall list settings must be configured to explicitly prevent all types of connections between network components and allow only needed list based on user request and business needs while reviewing such lists periodically.
12- Mechanisms for DNS security must be implemented.
13- Intrusion Prevention Systems (IPS) such as IDS/IPS, HIDS/HIPS to network segments must be implemented and review them regularly.
14- Network Advanced Persistent Threat (APT) protection systems must be provided on the network of critical systems and update it continuously.
15- Distributed Denial of Service Attack (DDoS) systems on systems must be provided and updated on an ongoing basis.
16- Appropriate techniques to protect the channel used for networking with the cloud computing service provider must be used.
17- The use of network communications, services, and contact points between different zones must be restricted and limited in order to the minimum to meet operation, maintenance and safety requirements.

18- Firewall rules configurations must be reviewed on an annual basis, and critical systems networks firewall at least on a bi-annual basis

19- Blacklist of malicious IP addresses and websites must be developed, updated, and blocked.

20- Connecting Wi-Fi network to the MCS internal network must be prevented without a full study of associated risks, the use of safe authentication and encryption methods, protection of private technology assets, data confidentiality and integrity along with protection of MCS systems and applications.

21- Connecting critical systems to the MCS wireless network must be prevented.

22- Connecting devices to critical systems of local networks must be prevented before they get inspected to ensure they meet minimum security requirements for critical systems.

23- The internal and external network of MCS must be evaluated while ensuring the organization network cybersecurity risks match the risks appetite periodically at least once a year.

24- Appropriate techniques to decrypt the web traffic (SSL/HTTPS Inspection) must be provided.

25- Remote access and connection must be restricted to critical systems only when needed, while providing up-to-date and secure mechanisms, protocols, and technologies to ensure secure connection (e.g. VPN, Site-to-Site VPN).

26- Only whitelisting for critical systems firewall rules must be allowed.

4.5 Physical and Environmental Security

1- House network computer equipment must be in a controlled and secure environment and ensure temperature and humidity are set at a certain degree in addition to availability of uninterruptible power supply "UPS".

2- Physical access to network devices must be restricted to authorized users only to protect such devices against theft or tamper.

3- All access cases must be recorded and maintain related logs in addition to monitoring network device areas using CCTV with continuous monitoring.

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- The Cybersecurity Department and the Information Technology Department 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 2-5-1 Network Security Management