Cybersecurity Management		
Server Security Policy		
Doc: MCS-CS-POL-26	Issue/Rev: 1.0	Date: 21.12.2024

Server Security Policy

MCS Cybersecurity Department

Cybersecurity Management		
Server Security Policy		
Doc: MCS-CS-POL-26	Issue/Rev: 1.0	Date: 21.12.2024

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	Server 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
- **SIEM:** Security Information and Event Management: A system used to collect and analyze security-related data from various sources.
- **MFA:** Multi-Factor Authentication, A security system that requires more than one method of authentication to verify user identity.
- **KPIs:** Key Performance Indicators, Metrics used to evaluate the effectiveness and performance of a particular process or activity.
- **VPN:** Virtual Private Network, A network technology that creates a secure, encrypted connection over a less secure network (e.g., the Internet).
- **VAPT:** Vulnerability Assessment and Penetration Testing
- **Firewall:** A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

2 PURPOSE

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

4 POLICY STATEMENTS

4.1 General Requirements

1- All MCS's servers must be identified, listed, and recorded under a specific operational team that is responsible for the operational and security processes as per MCS's policies and other relevant legal and regulatory requirements.
2- Server technical security standards must be developed, documented, approved, and reviewed for the servers used within MCS in line with the best international practices, MCS's approved policies and regulatory procedures, and other relevant legal and regulatory requirements.
3- Servers must be configured based on approved technical security standards before their deployment in the production environment.
4- Server backups must be performed regularly as per MCS's approved Backup Management Policy to ensure their recovery in case of an accidental incident or damage.
5- Necessary security technologies must be used to securely decommission and reuse servers containing classified information as per the relevant policies and legal and regulatory requirements.
6- Server software including operating systems and application software must be kept up to date, and the latest security patches and fixes must be applied according to MCS's approved Patch Management Policy.
7- Key Performance Indicators (KPIs) must be used to ensure the continuous improvement and effective and efficient use of the server protection requirements.

4.2 Server Configuration

1- MCS's approved secure configuration and hardening requirements must be applied.
2- Inactive servers and applications must be decommissioned as per the approved technical security standards.
3- Secure configuration and hardening for servers must be approved, reviewed, and updated annually and every six months for critical systems' servers.
4- Static passwords of servers must be changed as per MCS's approved technical security standards.

4.3 Access and Administration

1- Access to MCS's servers must be restricted to authorized users and when needed only.
2- Access to critical systems and servers must be restricted to System Administrators' accounts. Administrators' accounts and privileges must be reviewed periodically as per MCS's approved Identity and Access Management Policy.
3- Access to critical systems' servers must be restricted and limited to the technical team that has privileged access and via workstations only, while prohibiting the use of laptops. These workstations must be isolated in a management network and must not be connected to any other network or service (e.g., email or the Internet).
4- Access to critical systems' servers must require Multi-Factor Authentication (MFA).
5- Factory and default accounts must be disabled or changed, and unused services and ports in the operating system must be disabled on all servers.
6- Data stored on servers must be protected and encrypted in line with MCS's approved Cryptography Policy, based on the data classification type and according to the relevant legal and regulatory requirements.

4.4 Server protection

1- Outdated and unreliable servers must not be permitted to connect to MCS's network. They must be put in an isolated network to install the required updates in order to minimize related cybersecurity risks that might lead to unauthorized access, malware infections, or data leakage.
2- Modern and advanced protection technologies and mechanisms must be used and managed securely on all servers to protect them against viruses, suspicious activities, malware, and Zero-Day attacks.
3- Only specific application and software execution files must be whitelisted on critical systems' servers.
4- The use of external storage media on servers must be restricted. Cybersecurity Department’s prior authorization must be obtained before using such media, and their secure usage must be ensured.
5- Servers must be installed in an appropriate area in the network structure/diagram as determined according to legal and regulatory requirements to ensure their effective management and protection.

4.5 Server Management Operational Requirements

1- Servers must be managed centrally in MCS to detect risks promptly and facilitate server management and monitoring through restricting access, patching, etc.
2- Servers in virtual environments must be protected and securely managed based on cybersecurity risk assessments.

3- Servers must be configured to forward logs to a Security Information and Event Management (SIEM) system as per MCS's approved Cybersecurity Events Log Management and Monitoring Management Policy.
4- Clock synchronization shall be performed centrally for all servers according to an accurate, approved, and reliable source.
5- All the needed requirements to operate servers properly and securely must be provided, such as providing an appropriate and secure environment and monitoring and restricting physical access to server zones to the authorized personnel only.
6- The Information Technology Department must monitor operational servers and ensure their performance effectiveness, availability, storage sufficiency, etc.

4.6 Vulnerability Management and Penetration Testing

1- Servers must be periodically scanned for vulnerabilities, and discovered vulnerabilities must be remediated based on their classification and the associated cybersecurity risks, as per MCS's approved Vulnerability Management Policy and according to the relevant legal and regulatory requirements.
2- Penetration tests must be conducted periodically on all servers, as per MCS's approved Penetration Testing Policy.
3- Security patches and fixes must be deployed to remediate vulnerabilities and increase server efficiency and security as per MCS's approved Patch Management Policy.

4.7 Server Physical and Environmental Security

1- Access to and exit from MCS’s server facilities must be monitored and controlled, using for example doors, physical locks, and modern surveillance systems.
2- Environmental factors such as heat, air conditioning, and smoke, as well as fire alarm systems and firefighting systems, must be monitored and controlled.
3- Physical isolation must be applied to servers and critical systems' networks in an access-restricted environment as per the relevant policies and legal and regulatory requirements.
4- Proper physical security controls must be implemented (e.g., security monitoring cameras inside and outside MCS’s data centers, security guards, secured cables, etc.).

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