Cybersecurity Management		
Database Security Policy		
Doc: MCS-CS-POL-16	Issue/Rev: 1.0	Date: 22.12.2024

Database Security Policy

MCS Cybersecurity Department

Cybersecurity Management		
Database Security Policy		
Doc: MCS-CS-POL-16	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	Database Security Policy	22.12.2024

Cybersecurity Management		
Database Security Policy		
Doc: MCS-CS-POL-16	Issue/Rev: 1.0	Date: 22.12.2024

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
- **DBMS:** Database Management System
- **Database Administrators:** Professionals responsible for managing and securing databases, ensuring performance, and handling backups
- **Multi-Factor Authentication:** A security process where users must provide two or more verification factors to gain access to a system
- **SSH:** Secure Shell Protocol, A network protocol used to securely access and manage devices over an unsecured network
- **VPN:** Virtual Private Network, A method used to securely connect to a remote network, ensuring data privacy and encryption
- **SSL:** Secure Sockets Layer, A standard security technology for establishing an encrypted link between a server and a client
- **TLS:** Transport Layer Security, A protocol that ensures privacy between communicating applications, widely used to secure data transmitted over the internet
- **KPI:** Key Performance Indicator, A metric used to evaluate the effectiveness of an organization in achieving key objectives
- **SLAs:** Service Level Agreements, Contracts between a service provider and client, defining the level of service expected from the provider

- **Cryptography:** The practice of securing communication and data by converting it into a secure format using algorithms and keys
- **Hashing:** A process of converting data into a fixed-size string of characters, which typically represents the data's unique identifier
- **Patch Management:** The process of managing and applying updates to software systems, especially to address security vulnerabilities or bugs
- **Event Logs:** Logs that record activities and transactions in a system, used to monitor and troubleshoot potential issues or security threats

2 PURPOSE

This policy aims to define the cybersecurity requirements related to the protection of MCS's databases 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 Database Management Systems (DBMSs)) and applies to all personnel (employees and contractors) in the MCS.

4 POLICY STATEMENTS

4.1 General Requirements

1- DBMSs used in MCS must be defined and documented.
2- A proper secure environment must be provided for DBMSs to protect them against operational and environmental risks in line with database classification.
3- DBMSs technical security standards for MCS's DBMSs must be developed and approved, and they must be implemented by the Database Administrators (DBAs).
4- Users' direct access to and handling of databases must be restricted to DBAs only and through applications only based on authorized access while implementing security solutions that limit or prohibit DBAs from accessing classified data, as per MCS's approved Identity and Access Management Policy.
5- Database access, review, or modification privileges must be granted according to MCS's approved Identity and Access Management Policy.
6- The requirements of all MCS's approved policies related to configuration and hardening security must be implemented, including but not limited to the following policies:
   - MCS's approved Server Protection Policy.

- MCS's approved Malware Protection Policy.
- MCS's approved Physical Security Policy.

7- Copying or transferring the data of critical systems' databases from the production environment to any other environment must be prohibited unless the necessary tests are conducted.
8- Key Performance Indicators (KPIs) must be used ensure the continuous improvement and effective and efficient use of the database protection requirements.

4.2 Database Hosting Security Requirements

1- Business continuity and disaster recovery requirements must be defined for hosted databases in the relevant contracts with the cloud service providers as well as including respective roles and responsibilities regarding plans, backup tests, incident response, and disaster recovery, etc.
2- Logical and physical isolation must be provided between MCS's databases and other hosted databases, especially for critical databases, in line with database classification.
3- The secure configuration and hardening of MCS's databases must be reviewed periodically, at least once every year.
4- Administrative access to databases must be restricted using a solid encryption method, such as the Secure Shell Protocol (SSH), Virtual Private Networks (VPN), the Secure Sockets Layer (SSL),Transport Layer Security (TLS), or a Multi-Factor Authentication (MFA), as per MCS's approved Cryptography Policy.

4.3 DBMS Change Management Requirements

1- Changes to databases (such as database migration and transfer to a production environment) must follow MCS's approved change management process.
2- DBMS must be patched and updated as per MCS's approved Patch Management Policy.
3- Trusted, approved, and licensed DBMSs must be used upon update or change.
4- A clear DBMS disaster recovery plan must be in place, and it must be reviewed and tested annually.
5- Service Level Agreements (SLAs) must be signed with vendors for DBMSs in the production environment.
6- Hashing and encryption must be applied to databases during transmission and storage as per MCS's approved Classification Policy and Cryptography Policy.

4.4 DBMS Event Log Monitoring

1- DBMS event logs must be enabled and maintained as per MCS's approved Cybersecurity Event Logs and Monitoring Management Policy.
2- Cybersecurity Department must consistently monitor database event logs and users' behavior.

3- Cybersecurity Department must consistently monitor DBA-related event logs and behavior and review them every six months at least.

4.5 Operational Requirements

1- Information Technology Department must monitor operational DBMSs, and ensure the quality of their performance, their availability, and the availability of sufficient storage capacity, etc. It must also back up the databases.
2- Clock Synchronization must be ensured centrally for all DBMSs.
3- The requirements of MCS's approved Backup and Recovery Policy must be implemented.

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 2-7-1 Data and Information Protection