



Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Identity and Access Management Policy			
Doc: MCS-CS-POL-19	Issue/Rev: 1.0	Date: 21.12.2024	

# Identity and Access Management Policy

MCS Cybersecurity Department

Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Identity and Access Management Policy			
Doc: MCS-CS-POL-19	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	Identity and Access Management Policy	21.12.2024

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals &amp; Services Company</div></div>
Identity and Access Management Policy			
Doc: MCS-CS-POL-19	Issue/Rev: 1.0	Date: 21.12.2024	

## TABLE OF CONTENTS

<b>1</b>	<b>ABBREVIATIONS &amp; DEFINITIONS .....</b>	<b>4</b>
<b>2</b>	<b>PURPOSE .....</b>	<b>4</b>
<b>3</b>	<b>SCOPE.....</b>	<b>5</b>
<b>4</b>	<b>POLICY STATEMENTS .....</b>	<b>5</b>
4.1	GENERAL REQUIREMENTS .....	5
4.2	GRANTING ACCESS.....	6
4.2.1	<i>User Accounts Access Requirements .....</i>	<i>6</i>
4.2.2	<i>Privileged Access Requirements .....</i>	<i>7</i>
4.2.3	<i>Remote Access to MCS's Networks .....</i>	<i>7</i>
4.2.4	<i>Revoking and Changing Access .....</i>	<i>7</i>
4.2.5	<i>Identity and Access Management Review .....</i>	<i>8</i>
4.2.6	<i>Password Management.....</i>	<i>8</i>
4.2.7	<i>Password Protection.....</i>	<i>8</i>
<b>5</b>	<b>ROLES AND RESPONSIBILITIES.....</b>	<b>9</b>
<b>6</b>	<b>UPDATE AND REVIEW .....</b>	<b>9</b>
<b>7</b>	<b>COMPLIANCE .....</b>	<b>9</b>
<b>8</b>	<b>REFERENCES .....</b>	<b>9</b>

Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Identity and Access Management Policy			
Doc: MCS-CS-POL-19	Issue/Rev: 1.0	Date: 21.12.2024	

## 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, 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, A measurable value used to evaluate the effectiveness of cybersecurity controls
- **MFA:** Multi-Factor Authentication, Security mechanism requiring two or more verification factors to access a system
- **Active Directory (AD):** Microsoft service for identity and access management within an organization
- **Segregation of Duties (SoD):** Concept of separating tasks and privileges to reduce fraud and errors
- **Cybersecurity Event Logs:** Records of security-related activities used for monitoring and auditing
- **SNMP:** Simple Network Management Protocol, Used for managing and monitoring network devices, requiring secure configurations

## 2 PURPOSE

This policy aims to define the cybersecurity requirements related to identity and access management for MCS's information and technology assets, in order to minimize the cybersecurity risks resulting

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات</div><div>Modern Chemicals &amp; Services Company</div></div>
Identity and Access Management Policy			
Doc: MCS-CS-POL-19	Issue/Rev: 1.0	Date: 21.12.2024	

from internal and external threats in MCS and ultimately preserving 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 information and technology assets in the MCS and applies to all personnel (employees and contractors) in the MCS.

### 4 POLICY STATEMENTS

#### 4.1 General Requirements

- 1- An access management procedure must be documented and approved to illustrate, monitor, and implement the creation, modification, and revocation of access privileges to MCS's information and technology assets.
- 2- Users' identities must be created according to MCS's legal and regulatory requirements.
- 3- User authentication and validation must be performed using a username and password before granting users access to MCS's information and technology assets.
- 4- Users' identities, accounts, and privileges must be kept confidential, and users (personnel, third parties, and other users) must be required to maintain the privacy of such information.
- 5- An authorization matrix must be documented, approved, and reviewed based on the following identity and access management principles:
  - Need to know and need to use.
  - Segregation of duties.
  - Least privilege.
- 6- Authentication controls for all information and technology assets in MCS must be implemented via an automated and centralized access control system, such as Domain services -Active Directory.
- 7- Generic user accounts must not be allowed to access MCS's information and technology assets.
- 8- Secure session management must be ensured, including session authenticity, logout, and timeout.
- 9- Systems and sessions must be configured to automatically timeout after a specific period (Session Timeout), as per MCS's approved Identity and Access Management Standard.
- 10- Systems and sessions must be configured to temporarily logout after a specific number of unsuccessful login attempts, as per MCS's approved Identity and Access Management Standard.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات</div><div>Modern Chemicals &amp; Services Company</div></div>
Identity and Access Management Policy			
Doc: MCS-CS-POL-19	Issue/Rev: 1.0	Date: 21.12.2024	

- 11- Users' accounts that have been inactive for a specific period must be disabled, as per MCS's approved Identity and Access Management Standard.
- 12- All identity and access management systems must be configured to forward logs to a central logging and monitoring system as per the Cybersecurity Event Logs and Monitoring Management Policy.
- 13- Direct access to and handling of critical systems' databases must not be granted to users; except Database Administrators which can access the databases only through the applications. Procedures must be in place to prevent Database Administrators from accessing classified and sensitive data, as per MCS's approved Database Security Policy.
- 14- Procedures to manage service accounts must be documented and approved. Service accounts between applications and systems must be periodically reviewed and securely managed, and interactive users' access through Interactive Login must be disabled.
- 15- Users' privileges for remote work must be managed based on business needs, considering system criticality, privilege levels, and the types of devices used by personnel to work remotely, in line with the relevant legal and regulatory requirements.
- 16- Key Performance Indicators (KPIs) must be used to ensure the continuous improvement and efficient and effective use of identity and access management protection requirements.

## 4.2 Granting Access

### 4.2.1 User Accounts Access Requirements

- 1- Access must be granted based on the user request by an approved form from Cybersecurity Department or by the approved system from the line manager and the system owner. The request must define the system name, request type, access type, privilege, and duration (in case the access privilege is temporary).
- 2- Access to any of MCS's information and technology assets must be granted in line with the roles and responsibilities of the user, after obtaining the required approvals.
- 3- User IDs must be created following a standardized naming convention format that enables tracking the activities conducted by the user ID and linking them with the user (e.g., <first name initial> dot <last name>, or a pre-defined employee number with the Human Resources Department).
- 4- Concurrent logins from multiple workstations must be disabled.
- 5- The number of allowed unsuccessful login attempts to the system must be defined to prevent password guessing attacks as per MCS's approved Identity and Access Management Standard.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات</div><div>Modern Chemicals &amp; Services Company</div></div>
Identity and Access Management Policy			
Doc: MCS-CS-POL-19	Issue/Rev: 1.0	Date: 21.12.2024	

#### 4.2.2 Privileged Access Requirements

In addition to the controls stipulated in the “User Accounts Access Requirements” section, the below controls must be applied to privileged accounts:

- 1- Administrator privileges must be assigned based on job duties, while taking into account the segregation of duties principle.
- 2- Password history must be enabled to track the number of passwords that have been changed.
- 3- Default accounts, specifically privileged ones such as “Root”, “Admin”, and “Sys id”, must be renamed.
- 4- Privileged accounts must be prevented to be used for day-to-day operations and connected to the Internet.
- 5- Privileged users' accounts on information and technology assets must be authenticated through a Multi-Factor Authentication (MFA) mechanism, using at least two factors, as per MCS's approved Identity and Access Management Standard.
- 6- A Privileged Access Management (PAM) solution must be used to maintain and manage privileged accounts.
- 7- Access to critical systems and the systems that are used to manage and monitor critical systems must require an MFA mechanism for all personnel.

#### 4.2.3 Remote Access to MCS's Networks

- 1- Remote access to information and technology assets must be granted after obtaining permission from the Cybersecurity Department, and it must be restricted using an MFA mechanism through secure channels that are approved in MCS.
- 2- Event logs of remote access sessions must be maintained, and related activities must be monitored continually based on the criticality of information and technology assets.

#### 4.2.4 Revoking and Changing Access

- 1- The Human Resources Department must notify the Information Technology Department to take necessary actions when a user is transferred, assigned new duties, or when the user's contract with MCS ends or is terminated. The Information Technology Department must revoke or update the user's account and access based on the newly assigned role. These measures must be automated as much as possible.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات</div><div>Modern Chemicals &amp; Services Company</div></div>
Identity and Access Management Policy			
Doc: MCS-CS-POL-19	Issue/Rev: 1.0	Date: 21.12.2024	

- 2- The event logs of user whose access is revoked must be prohibited of deletion, and they must be maintained as per MCS's approved Cybersecurity Event Logs and Monitoring Management Policy.

#### 4.2.5 Identity and Access Management Review

- 1- User IDs and their use for information and technology assets must be reviewed annually. User IDs and their use for critical systems must be reviewed at least every three months.
- 2- User profiles and their use for information and technology assets must be reviewed annually. User profiles and their use for critical systems must be reviewed at least every three months.

#### 4.2.6 Password Management

- 1- A secure password policy with high standards must be applied for all accounts in MCS, as per its approved Identity and Access Management Standard in MCS and other relevant legal and regulatory policies and requirements.
- 2- Users must be notified before the expiration of their passwords to remind them to change their passwords before the expiration.
- 3- Previously used passwords must not be used.
- 4- All information and technology assets must be configured to force users to change their temporary passwords upon their first login.
- 5- Default passwords for all information and technology assets must be changed before their deployment to the production environment.
- 6- Simple Network Management Protocol (SNMP) default community strings (such as "public," "private" and "system") must be changed and must be different from the passwords used to log into the respective technology assets.

#### 4.2.7 Password Protection

- 1- All MCS's information and technology asset passwords must be encrypted to be rendered unreadable during entry, transmission, and storage as per MCS's approved Cryptography Policy.
- 2- Passwords must be masked on the screen when being entered.
- 3- "Remember Password" feature must be disabled on MCS's systems and applications.
- 4- Dictionary words must not be allowed to be used as is in the passwords.
- 5- Passwords must be delivered to users using a secure and reliable method following defined and approved procedures.
- 6- If a user requests a password reset by phone, Internet, or any other method, the user's identity must be authenticated before resetting the password through

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals &amp; Services Company</div></div>
Identity and Access Management Policy			
Doc: MCS-CS-POL-19	Issue/Rev: 1.0	Date: 21.12.2024	

defined and approved methods, including but not limited to activating and updating security questions.

- 7- The passwords of privileged accounts and service accounts must be protected and stored securely in a proper location (in a sealed envelope in a safe box) or using a Privilege Access Management (PAM) solution.

## 5 ROLES AND RESPONSIBILITIES

- 1- **Policy Owner:** Cybersecurity Manager
- 2- **Policy Review and Update:** Cybersecurity Department
- 3- **Policy Implementation and Execution:** Information Technology Department, Human Resources 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 2-2-1 Identity and Access Management