Cybersecurity Management		
Backup Policy		
Doc: MCS-CS-POL-03	Issue/Rev: 1.0	Date: 20.12.2024

Backup Policy

MCS Cybersecurity Department

Cybersecurity Management		
Backup Policy		
Doc: MCS-CS-POL-03	Issue/Rev: 1.0	Date: 20.12.2024

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	Backup Policy	20.12.2024

Cybersecurity Management		
Backup Policy		
Doc: MCS-CS-POL-03	Issue/Rev: 1.0	Date: 20.12.2024

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
- **OT:** Operational Technology
- **ICS:** Industrial Control Systems
- **SIS:** Safety Instrumented Systems
- **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
- **L1 (Level 1 - Machine Control):** This level includes sensors, actuators, Programmable Logic Controllers (PLCs), and other devices that directly control industrial machines and processes.
- **L2 (Level 2 - Process Monitoring):** Supervisory Control and Data Acquisition (SCADA) and Human-Machine Interfaces (HMI) used for monitoring and controlling industrial operations.
- **L3 (Level 3 - Production Management):** Manufacturing Execution Systems (MES) and other software used for production planning, scheduling, and efficiency optimization.

2 PURPOSE

This policy aims to define the cybersecurity requirements related to the backup and recovery of all of MCS's information and technology assets 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 (e.g., systems, data and information) and applies to all personnel (employees and contractors) in the MCS.

4 POLICY STATEMENTS

4.1 General Requirements

1- Install Server for Backups and it shall be encrypted and stored in a secured physically separate location.
2- Provide a disaster recovery plan that is periodically tested.
3- Files, devices, data, and procedures available for use in case of failure or loss, or in case of deletion or suspension of their original copies.
4- A method of storage in which the backup is regularly taken on a remote server over a network, (either within the organization's network or hosted by a service provider).
5- Scope and coverage of backups to cover critical technology and information assets.
6- Ability to perform quick recovery of data and systems after cybersecurity incidents.
7- Periodic tests of backup's recovery effectiveness.
8- Backups for all OT/ICS assets must be covered and stored in centralized and offline locations. This is for all levels: L1, L2,L3.
9- Assets' critical configuration files and engineering files must be included in the backup's scope. This is for all levels: L1, L2,L3
10- Backups must be performed periodically as per the de- fined OT/ICS assets classification and their associated risks. This is for all levels: L1, L2,L3.
11- Access, storage, and transfer of backups and their mediums must be secured to ensure their protection against damage, change, or unauthorized access. This is for all levels: L1, L2,L3.
12- Strict limitation must be enforced on the physical access to all OT/ICS assets, including Safety Instrumented Systems (SIS). This is for all levels: L1, L2
13- Visitor access records to restricted locations where OT/ ICS reside must be maintained. This is for all levels: L1, L2,L3.
14- Work being performed by contractor or vendor personnel must be monitored. This is for all levels: L1, L2

15- Trainings and skillsets for the organizational security guards must be provided in line with roles and responsibilities with respect to OT/ICS physical security. This is for all levels: L1, L2,L3.
16- Physical security capabilities and readiness must be peri- odically tested by performing simulation exercises (such as social engineering). This is for all levels: L1, L2
17- The cybersecurity requirements for physical security in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically. This is for all levels: L1, L2.

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 2-9-1 Backup and Recovery Management