


Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Workstations, Mobile Devices and BYOD Security Policy			
Doc: MCS-CS-POL-31	Issue/Rev: 1.0	Date: 21.12.2024	

Workstations, Mobile Devices and BYOD Security Policy

MCS Cybersecurity Department

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Workstations, Mobile Devices and BYOD Security Policy			
Doc: MCS-CS-POL-31	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	Workstations, Mobile Devices and BYOD Security Policy	21.12.2024


Cybersecurity Management			<div> الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div>
Workstations, Mobile Devices and BYOD Security Policy			
Doc: MCS-CS-POL-31	Issue/Rev: 1.0	Date: 21.12.2024	

TABLE OF CONTENTS

1	ABBREVIATIONS & DEFINITIONS	4
2	PURPOSE	5
3	SCOPE.....	5
4	POLICY STATEMENTS	5
4.1	GENERAL REQUIREMENTS	5
4.2	WORKSTATIONS CYBERSECURITY REQUIREMENTS	7
4.3	MOBILE DEVICES CYBERSECURITY REQUIREMENTS	7
4.4	BOYD CYBERSECURITY REQUIREMENTS.....	8
5	ROLES AND RESPONSIBILITIES.....	8
6	UPDATE AND REVIEW	8
7	COMPLIANCE	8
8	REFERENCES	8

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Workstations, Mobile Devices and BYOD Security Policy			
Doc: MCS-CS-POL-31	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
- **BYOD:** Bring Your Own Device
- **Privileged Access Workstations:** Dedicated workstations for privileged access users, isolated for security.
- **Data Leakage Prevention:** A security strategy to prevent unauthorized access, leakage, or loss of data.
- **End of Life (EOL):** The point at which a product or software is no longer supported or updated by the vendor.
- **Key Performance Indicator (KPI):** A measurable value used to track the success or progress of a certain goal.
- **Transport Layer Security (TLS):** A cryptographic protocol to secure communication over a computer network.
- **Open Web Application Security Project:** A community-driven organization focused on web application security.
- **Web Application Firewall:** A security tool that filters and monitors HTTP traffic to and from a web application.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Workstations, Mobile Devices and BYOD Security Policy			
Doc: MCS-CS-POL-31	Issue/Rev: 1.0	Date: 21.12.2024	

2 PURPOSE

This policy aims to define the cybersecurity requirements related to the use of workstations, mobile devices and privately owned devices (“Bring Your Own Device” BYOD) within MCS to minimize the cybersecurity risks resulting from internal and external threats 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 applies to all MCS systems, applications and software codes that are designed and developed in-house or using third parties, with a target audience of MCS’s personnel (employees and contractors).

4 POLICY STATEMENTS

4.1 General Requirements

- 1- Data and information stored on workstations, mobile devices and BYOD must be protected as per their classification by the appropriate security controls to restrict access to such information and prevent access or viewing by unauthorized personnel.
- 2- Update workstations, mobile devices and BYOD software including operating systems, programs, and applications and implement the latest security patches must be according to the Patch Management Policy approved by MCS.
- 3- Implement secure configuration and hardening controls to workstations, mobile devices and BYOD must be in accordance with Cybersecurity Standards approved by MCS.
- 4- Personnel must not be granted privileged access to MCS systems using mobile devices and BYOD. Any access must be given following the Principle of Least Privilege.
- 5- Operating system and application default user accounts must be disabled or removed.
- 6- All workstations, mobile devices and BYOD must be centrally synchronized (Clock Synchronization) from an accurate and reliable source.
- 7- Workstations and mobile devices must be configured with an authorized use Banner.
- 8- Only whitelisted applications must be allowed on workstations and mobile devices.
- 9- Data Leakage Prevention must be used as well as data monitoring systems to ensure data protection on workstations and mobile devices.
- 10- Full Disk Encryption must be applied to privileged, advanced and critical systems access workstations and mobile devices storage media according to the MCS Cryptography Standard.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Workstations, Mobile Devices and BYOD Security Policy			
Doc: MCS-CS-POL-31	Issue/Rev: 1.0	Date: 21.12.2024	

- 11- The use of external storage media must be restricted according to the MCS's procedures after obtaining a prior permission from Cybersecurity Department.
- 12- Mobile devices and BYOD must be centrally managed by using Mobile Device Management (MDM).
- 13- Workstations, mobile devices and BYOD with end-of-life software including operating systems and application software must not be permitted to connect to MCS's network to prevent security threats arising from unpatched end-of-life software.
- 14- Workstations, mobile devices and BYOD without up-to-date security software must be prevented from connecting to MCS's network to avoid cyber threats causing unauthorized access, malware infections or data exfiltration. Protection software include mandatory software such as Antivirus, Anti-malware, Host-Based Firewall and Host-Based Intrusion Detection/Prevention.
- 15- Deviations from acceptable user behaviour, risk assessment, and development and/or recommendation of appropriate countermeasures must be defined to mitigate them.
- 16- Unattended workstations and mobile devices must be configured to show a privacy screensaver protected with a password in case of Session Timeout for 5 minutes.
- 17- Workstations and mobile devices accounts must be centrally managed through the Active Directory server of the MCS's domain or Central Management System.
- 18- MCS's appropriate Group Policy must be enforced and applied on all workstations and mobile devices to ensure secure configuration and hardening and the organization compliance to regulatory and security controls, in addition to installing the necessary software.
- 19- A regular backup of data stored on workstations and mobile devices must be performed as per MCS's Backup and Recovery Policy.
- 20- Techniques that allow the remote removal of data stored on mobile devices and BYOD must be provided and used under the following circumstances:
 - Mobile device is lost or stolen.
 - Upon end or termination of user employment at MCS.
 - Expiration of use and delivery of the mobile device to the concerned department MCS.
- 21- Telework systems and information devices must be protected through the following:
 - Implement Secure Session Management that includes session's authenticity, lockout, and timeout
 - Implement security patches on telework systems, at least once a month
 - Review telework systems protection configurations and hardening at least once a year.
 - Restrict enabling telework features and services on an as-needed basis, provided that potential cyber risks are assessed in case of need to enable them.
- 22- Awareness campaigns must be conducted on the safe ways to use mobile devices and BYOD as well as users' responsibilities in accordance with the Acceptable Use Policy

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Workstations, Mobile Devices and BYOD Security Policy			
Doc: MCS-CS-POL-31	Issue/Rev: 1.0	Date: 21.12.2024	

approved by MCS, in addition to awareness campaigns dedicated to privileged access users.

- 23- Workstations, mobile devices and BYOD security procedures and criteria must be developed based on the work need.
- 24- Key performance indicators must be used to ensure the continuous improvement and proper and effective use of workstations, mobile devices and BYOD requirements.

4.2 Workstations Cybersecurity Requirements

- 1- Privileged access workstations must be dedicated to privileged technical team and must be isolated and connected to a dedicated Management Network without connection to any other network or service.
- 2- Privileged access workstations (PAWs) must be configured to forward logs to MCS central logging and monitoring system as per MCS Event Logs and Monitoring Management Policy and it cannot be reconfigured by user.
- 3- Workstations must be physically safeguarded within the buildings of MCS and facility entry/exit must be registered after obtaining the necessary approvals as per MCS Physical Security Policy.
- 4- Protection of workstations from viruses, malware, advanced persistent threats (APTs), zero-day attacks and any other type of malicious attacks must be ensured through Endpoint Protection Software.
- 5- Integrity, availability and recoverability of workstation data must be ensured against tampering, accidental loss or damages.
- 6- All necessary security controls must be applied when removing workstations data, especially those connected to cloud services, as per MCS Data and Information Protection Policy.
- 7- Patches must be managed at least once a month for devices used to manage external and connected critical systems and at least once every three months for devices used to manage internal critical systems, as per MCS's change management policy.
- 8- Configurations of devices used to manage critical systems must be reviewed and hardened at least once every six months.

4.3 Mobile Devices Cybersecurity Requirements

- 1- Mobile devices access to critical systems must be restricted only for a short period of time after conducting risk assessments and obtaining the necessary approvals from Cybersecurity Department.
- 2- It must be ensured that unattended, lost and/or stolen devices cannot be accessed by unauthorized users (Device Access Locking).
- 3- The integrity of information stored on mobile devices (Device Contents Integrity) must be ensured.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Workstations, Mobile Devices and BYOD Security Policy			
Doc: MCS-CS-POL-31	Issue/Rev: 1.0	Date: 21.12.2024	

- 4- The operating system and applications installed on mobile devices must be properly updated and configured prior to use (Device OS and Applications Security) as per MCS technical standards.
- 5- Security patches for all mobile devices must be applied at least once a month.
- 6- Data and information of MCS stored on mobile devices must be encrypted and segregated.

4.4 BOYD Cybersecurity Requirements

- 1- In case workstations are used for business purposes, this must be supported by documented agreements with personnel along with technical security controls to protect MCS data and information.
- 2- Encrypt and segregate must be used for Data and information of MCS stored on mobile devices (BYOD).

5 ROLES AND RESPONSIBILITIES

- 1- **Policy Owner:** Cybersecurity Manager
- 2- **Policy Review and Update:** Cybersecurity Department
- 3- **Policy Implementation and Execution:** Information Technology 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 at 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 2-6-1 Mobile Devices Security