



Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Web Application Protection Policy			
Doc: MCS-CS-POL-30	Issue/Rev: 1.0	Date: 21.12.2024	

Web Application Protection Policy

MCS Cybersecurity Department

Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Web Application Protection Policy			
Doc: MCS-CS-POL-30	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	Web Application Protection Policy	21.12.2024


Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Web Application Protection Policy			
Doc: MCS-CS-POL-30	Issue/Rev: 1.0	Date: 21.12.2024	

TABLE OF CONTENTS

1	ABBREVIATIONS & DEFINITIONS	4
2	PURPOSE	4
3	SCOPE.....	5
4	POLICY STATEMENTS	5
4.1	GENERAL REQUIREMENTS	5
4.2	ACCESS RIGHT	6
4.3	SECURITY CONFIGURATION	6
5	ROLES AND RESPONSIBILITIES.....	7
6	UPDATE AND REVIEW	7
7	COMPLIANCE	7
8	REFERENCES	7

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Web Application Protection Policy			
Doc: MCS-CS-POL-30	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
- **OWASP:** Open Web Application Security Project
- **Web Application Firewall (WAF):** A security system that monitors and filters HTTP traffic to and from a web application to prevent attacks.
- **Multi-tier Architecture:** A system design principle that splits the architecture into layers (e.g., presentation, logic, data) to improve security, scalability, and maintainability.
- **Change Advisory Board (CAB):** A group responsible for approving changes to IT systems, including web applications, to ensure they meet security and operational requirements.

2 PURPOSE

This policy aims to define the detailed cybersecurity requirements related to the protection of MCS's external web applications 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 such as Essential Cybersecurity Controls (ECC-1:2018) and Critical Systems Cybersecurity Controls (CSCC-

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Web Application Protection Policy			
Doc: MCS-CS-POL-30	Issue/Rev: 1.0	Date: 21.12.2024	

1:2019) that are 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 external web applications and applies to all personnel (employees and contractors) in the MCS.

4 POLICY STATEMENTS

4.1 General Requirements

- 1- External web applications must be protected by a web application firewall (WAF) from external attacks.
- 2- External web applications must follow the (Multi-tier Architecture) principle, with at least (2-tier Architecture).
- 3- Critical external web applications must adopt and follow the (Multi-tier Architecture) principle, with at least (3-tier Architecture).
- 4- Only secure communication protocols (such as HTTPS, SFTP, TLS, etc.) must be used.
- 5- Development Environment and Testing Environment must be logically isolated from Production Environment.
- 6- Data and Information Protection techniques must be used in external web applications as per MCS approved Data and Information Protection Policy and Classification Policy.
- 7- Web applications purchased from third party vendors must adhere to MCS's cybersecurity policies and standards.
- 8- Minimum web applications and protection standards (OWASP Top Ten Web Application Security Risks) must be implemented for external web applications and critical systems.
- 9- Minimum application programming interface security standards (OWASP Top Ten API Security) must be implemented for external web applications of critical systems.
- 10- Web application cybersecurity architecture requirements must be defined to ensure that the web applications are designed and deployed in a secure manner.
- 11- It must be ensured that all web application event logs in MCS can be monitored and stored.
- 12- Integrity, availability and recoverability of web applications data against tampering, accidental loss or damages must be ensured through Backup and Archival.
- 13- Cybersecurity requirements for cloud-hosted web applications must be defined to ensure they are configured, installed and operated in a secure manner.
- 14- External web applications must be available and protected against Distributed Denial of Service "DDoS" Attacks at the applications and network level.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Web Application Protection Policy			
Doc: MCS-CS-POL-30	Issue/Rev: 1.0	Date: 21.12.2024	

15- Procedures and standards for web applications protection must be developed based on business need.

16- KPI must be used to ensure the continuous improvement and effective and efficient use of the Web Applications Protection requirements.

4.2 Access Right

- 1- Multi-factor Authentication must be implemented for user access to external web applications and system admins access to internal web applications.
- 2- Web applications development security standards, including but not limited to Secure Session Management, session authenticity, session logout, and session timeout, must be documented and approved.
- 3- Access to production systems must be restricted and controlled as per job responsibilities.
- 4- External web application users must be forewarned and acquainted of the Secure Usage Policy.
- 5- Secure means (Hashing Function) must be used to store user data when accessing external web applications such as a password.

4.3 Security Configuration

- 1- Cybersecurity Risk Assessments must be performed when planning the development or purchase of web applications prior to their deployment in production environment as per MCS's Cybersecurity Risk Management Policy.
- 2- Web application secure configuration and hardening requirements must be defined, reviewed and documented to ensure that the web applications are configured and operated in a secure manner.
- 3- Ensure confidentiality and integrity of web applications data as per MCS's Data and Information Protection Policy.
- 4- Prior to using classified information in testing environment, Cybersecurity Department's prior authorization must be obtained and restrict controls to protect such data, e.g. data scrambling and data masking, must be used and such data must be wiped immediately after that.
- 5- Source Code must be safeguarded and access to it or modification must be restricted to authorized users.
- 6- External web applications must undergo a Penetration Test in testing environment, results must be documented, and all vulnerabilities must be remediated before deployment in production environment as per MCS's Penetration Testing Policy.
- 7- Vulnerabilities Assessment must be performed for technology components of web applications and vulnerabilities must be remediated by installing MCS's patches on a regular basis.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Web Application Protection Policy			
Doc: MCS-CS-POL-30	Issue/Rev: 1.0	Date: 21.12.2024	

- 8- Tests must be conducted to assess Web applications protection in case of a new or Major Application Release, Acquired Web Applications, Point Releases, Patch Releases, and Emergency Releases.
- 9- Changes to web applications must be approved by the Change Advisory Board (CAB) before being launched into the production environment.

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 2-15-1 Web Application Security