



Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Secure Systems Development Life Cycle Policy			
Doc: MCS-CS-POL-25	Issue/Rev: 1.0	Date: 20.12.2024	

Secure Systems Development Life Cycle Policy

MCS Cybersecurity Department

Cybersecurity Management			<div> الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div>
Secure Systems Development Life Cycle Policy			
Doc: MCS-CS-POL-25	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	Secure Systems Development Life Cycle Policy	20.12.2024


Cybersecurity Management			 الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company
Secure Systems Development Life Cycle Policy			
Doc: MCS-CS-POL-25	Issue/Rev: 1.0	Date: 20.12.2024	

TABLE OF CONTENTS

1	ABBREVIATIONS & DEFINITIONS	4
2	PURPOSE	4
3	SCOPE.....	5
4	POLICY STATEMENTS	5
4.1	GENERAL REQUIREMENTS	5
4.2	SSDLC ADDITIONAL REQUIREMENTS	6
5	ROLES AND RESPONSIBILITIES.....	6
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>
Secure Systems Development Life Cycle Policy			
Doc: MCS-CS-POL-25	Issue/Rev: 1.0	Date: 20.12.2024	

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
- **SSDLC:** Secure Software Development Life Cycle, A process used for developing secure software, integrating security into every phase of development.
- **QA:** Quality Assurance, A way of preventing errors or defects in manufactured products and avoiding problems when delivering solutions or services.
- **End of Life (EOL):** Refers to the point in time when a software or hardware product is no longer supported, meaning no further updates or repairs are provided.
- **Secure Code Scanning:** A tool or process used to review development code to identify vulnerabilities, particularly those affecting sensitive data or critical applications.

2 PURPOSE

This policy aims to define cybersecurity requirements related to MCS's Secure Systems Development Life Cycle (SSDLC) process. The policy intends to set the appropriate requirements to govern MCS's systems and software development process in order to reduce the likelihood of cybersecurity attacks though poorly implemented designs and functionality. Integrating SSDLC good practices with MCS's Information Technology (IT) project and change management processes

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Secure Systems Development Life Cycle Policy			
Doc: MCS-CS-POL-25	Issue/Rev: 1.0	Date: 20.12.2024	

will help reduce the number, to mitigate the impact and to address the root cause of vulnerabilities in system designs, configurations and software packages.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to ECC-1:2018 and CCCC-1:2019, 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- All SSDLC activities must be managed in compliance with MCS's Information and Cybersecurity policies and related government regulations.
- 2- SSDLC policy and standards must be periodically reviewed and revised (as necessary) at least once a year.
- 3- SSDLC related training sessions and programs must be developed and delivered to relevant personnel.
- 4- An SSDLC project plan must be developed and tracked for progress against all MCS's IT design, development and implementation activities.
- 5- A secure and automated process for checking, approving and promoting newly developed or updated functionality must be leveraged by MCS for any software development activities.
- 6- Solution architecture and security must be developed and reviewed as part of all IT projects.
- 7- Baseline system security configurations must be applied to all MCS systems and devices.
- 8- Component interfaces required for product/feature development must be evaluated prior to integration.
- 9- Secure coding practices must be adhered to on all development projects and will align with industry best practices.
- 10- Testing and quality assurance activities must be performed across development activities and must be iterative in approach.
- 11- Software developed must be tested prior to being moved into the production environment.
- 12- Security vulnerability tests must be conducted for all critical systems and software in the MCS's IT environment.

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Secure Systems Development Life Cycle Policy			
Doc: MCS-CS-POL-25	Issue/Rev: 1.0	Date: 20.12.2024	

- 13- MCS must prepare a proper plan to deal with all software related vulnerabilities and the mitigation actions required based on the criticality.
- 14- Any IT project plans must ensure that deployment strategies are authorized, traceable and secure.
- 15- Any IT projects must be subjected to ongoing monitoring activities to measure and monitor project performance.
- 16- All software and applications must be subject to ongoing monitoring when designing and implementing software solutions.
- 17- All systems and software which reach end of life span or are no longer required by MCS must be decommissioned according to MCS security and media disposal policies.

4.2 SSDLC Additional Requirements

- 1- Security risk assessments must be carried out for all MCS systems, software and applications in accord with IT project, change management and security processes, as per related laws and regulations.
- 2- Threats to MCS systems, applications and software development projects must be identified and appropriately mitigated, as per related laws and regulations.
- 3- Security-related requirements including data classification and access controls must be integrated into the system or application software designs.
- 4- Systems and applications must be deployed securely into the production environment.
- 5- Network segregation and zoning for MCS system and application environments must be adhered to.
- 6- Data and information protection controls must be used in all MCS systems and applications.
- 7- A configuration and change management protocol must be adhered to and followed.
- 8- A secure code scanning tool must be used on development code to identify security vulnerabilities for sensitive data sets and critical applications.
- 9- Emergency change procedures must be developed and implemented.
- 10- Third party involvement in development activities must be formally identified and managed.
- 11- Compliance with MCS policies and standards for all IT projects must be adhered to.

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

Cybersecurity Management			<div><div>MCS</div><div>الشركة الكيميائية الحديثة للخدمات Modern Chemicals & Services Company</div></div>
Secure Systems Development Life Cycle Policy			
Doc: MCS-CS-POL-25	Issue/Rev: 1.0	Date: 20.12.2024	

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 1-6-3 Cybersecurity in Information and Technology Project Management