



Ministry of Digital Economy
and Entrepreneurship

ISO 27001 Maintenance ISMS Policy

Author: Haneen Emeir
Creation Date: 12-06-2020
Last Update Date: 09-12-2020
Version: 2.0
Classification: Public
Code: ISMS-MNG-01



ISMS Policy

Documentation Control

Approvals				
Name	Job Description	Party	Date	Signature
Sameera AL-Zoubi	Head of ISMS Committee	MoDEE	09 -12 - 2020	Attached in SC MoM, July 2020

Date	Author	Version	Change Reference	Approver
17.12.2019	IT Security C&T	1.0	Initial Release	ISMS SC
15.06.2020	Haneen Emeir	2.0	Review, Removed NITC	ISMS SC
09.12.2020	Haneen Emeir	2.0	Correct version number	ISMS SC

ISMS Policy

Introduction

Information security is a risk that has a very high impact on the entire organization, which may lead to disaster that effect on the national security. Consequently, building a policy that does not only cover the desired information security requirements but also defines other aspects such as: the objectives of the information security, ownership of policy, and delegation of duties will help in managing and responding for information security incidents properly.

1. Importance of Information Security

MoDEE have important data that must be protected. Moreover, implementing the ISMS policy is a requirement to implement public key infrastructure (PKI) the service which provide digital authentication capabilities for validating the identity of employees, citizens, and businesses.

2. Objective

The main objective of ISMS policy is to provide a controlled environment appropriate for carrying out MoDEE's mission and serving in achieving their strategy.

3. Scope

- ✓ The policy applies to all information created or received in **MoDEE**.
- ✓ This policy forms the basis of **MoDEE** Information Security Management System (ISMS) of related policies and procedures, based on the International Standard 27001, taking a risk-based approach to embed appropriate levels of information security controls and countermeasures.

4. Policy Statement

It is the policy of **MoDEE** to ensure that appropriate controls and countermeasures are put in place to protect corporate and client data, as well as the information technology systems, and services and equipment of **MoDEE**. The purpose of the policy is to protect **MoDEE's** information assets from all threats, whether internal or external, deliberate or accidental.

- ✓ **MoDEE** is committed to protect its information assets, personnel, intellectual property, computer systems, data, and equipment from all threats, whether internal or external, deliberate or accidental, in a cost-effective manner. This should be achieved with minimum inconvenience to authorized users and against threats to the level of service required by the **MoDEE** to conduct its business.
- ✓ **MoDEE** shall adopt ISO 27001 Information Security Management System (ISMS) as a tool to implement a formal system for protecting the confidentiality, integrity and availability of information.
- ✓ **MoDEE** is committed to comply with regulatory and legislative requirements.
- ✓ **MoDEE** is committed to satisfy the expectations and requirements of interested parties, and to provide the necessary resources to achieve this.
- ✓ Information security risks shall be managed based on **MoDEE's** approved risk management methodology.
- ✓ **MoDEE** is committed to treat and resolve security incidents and suspected vulnerabilities per their respective nature.
- ✓ Information security objectives will be defined based on the implemented risk assessment and will be monitored and reviewed by the **Information Security Management System Steering Committee (ISMS-SC)**.

5. Compliance Statement

ISMS Policy

Compliance with this policy and all other supporting policies, standards, and procedures is mandatory for all staff and third-parties. Violation of this policy or any other IS policies, standards, or procedures will result in corrective action by management. Disciplinary action will be consistent with the severity of the violation, as determined by an investigation, and as deemed appropriate by management.

6. Continual improvement

MoDEE should commit to:

- ✓ Encouraging information security improvements by engaging with its personnel, providing them with information security training and awareness, and enhancing their competences.
- ✓ Continually improve its ISMS and information security posture.
- ✓ Continually review this policy and its information security performance to ensure it improves over time.

7. Ownership

Information Security Management System Steering Committee (ISMS-SC) is the owner of this policy. Any changes or updates to the document shall be explicitly approved by the committee.

8. Delegation

Information Security Management System Steering Committee (ISMS-SC) delegate the authority for ISMS manager to create standards, procedures, and guidelines that implement this policy.

9. Availability

This policy is available to all **MoDEE** personnel and relevant interested parties. All **MoDEE** personnel are made aware of its commitment and the contents of this policy.