ARTAR

# ISMS Corporate Policy

## Information Security Management System Corporate Policy

Author: Dany Hallak

V2.0 Wednesday 15th of August, 2024

# ISMS Corporate Policy

| | |
|---|---|
| DOCUMENT CLASSIFICATION | Internal |
| DOCUMENT REF | ISMS-DOC-06-2 |
| VERSION | 2 |
| DATED | 15 August 2024 |
| DOCUMENT AUTHOR | Dany Hallak |
| DOCUMENT OWNER | Information Security Officer |

# Revision history

| VERSION | DATE | REVISION AUTHOR | SUMMARY OF CHANGES |
|---|---|---|---|
| V1 | 16 Feb 2022 | Dany Hallak | |
| V2 | 30 July 2023 | Dany Hallak | |
| V3 | 15 Aug. 2024 | Dany Hallak | |

# Distribution

| NAME | TITLE |
|---|---|
| ARTAR Employees | |
| | |
| | |

# Approval

| NAME | POSITION | SIGNATURE | DATE |
|---|---|---|---|
| Majed Al Jaber | Assist to CEO | | |
| Mohammad El Sayed | CFO | | |

| | | | |
|---|---|---|---|
| Tahseen Al Aktaa | CIO | | |

# Table of Contents

# 1 Purpose

Information security threats are a risk that has a very high impact on the entire organization. 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.

# 2 Policy Statement

It is the policy of ARTAR to ensure that appropriate controls and countermeasures are put in place to protect corporate and personnel data, as well as the information technology systems, and services and equipment of ARTAR.

a. ARTAR is committed to protect its information assets, personnel, 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 ARTAR to conduct its business.

b. ARTAR shall adopt ISO 27001 standard as a tool to implement a formal system for protecting the confidentiality, integrity, and availability of information.

c. ARTAR is committed to satisfy the information security expectations and requirements of interested parties, and to provide the necessary resources to achieve this.

d. Information security risks shall be managed based on ARTAR ’s approved risk management methodology.

e. 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.

f. ARTAR is committed to continually improve its ISMS through the implementation of the Plan – Do – Check – Act cycle.