

1 Purpose, Scope and Users

This Information Security Policy describes and establishes the scope and functioning of the information security within the Integrated Management System (IMS) - encompassing the Information Security Management System (ISMS / ISO 27001:2022), Quality Management System (QMS / ISO 9001:2015), data protection obligations (GDPR), and cybersecurity requirements (NIS2).

The IMS is developed and implemented jointly across the following legal entities: **LLC MOI Tech, LLC MOVI TECH-** in accordance with the requirements of ISO/IEC 27001:2022, ISO 9001:2015, GDPR, NIS2 and applicable laws of Ukraine .

The Policy defines **Company's** approach to information security management and has been disclosed to all personnel and counterparties in an appropriate and accessible form.

This Policy applies to the entire IMS, as defined in the IMS Scope Document. **This policy applies to all services, infrastructure and personnel of the MOI Tech group of companies.**

2 Reference Documents

- ISO/IEC 27001:2022, clauses 5.2 and 5.3
- IMS Scope Document
- Risk Analysis Procedure
- Statement of Applicability
- List of Legal, Regulatory and Contractual Requirements

3 Acronyms and Definitions

Term	Definition
Availability	The property of being accessible and usable on demand by authorised individuals, entities or processes.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities or processes.
Control	A concrete measure (including assigned responsibilities) which supports a control objective.
Control Objective	A statement describing the goal to be achieved by implementing controls.
Information	Any data, whether in electronic form, written on paper, spoken, or on any other medium.

Information Security	Preservation of confidentiality, integrity, and availability of information; may also include authenticity, accountability, non-repudiation and reliability.
ISMS	Information Security Management System (ISMS) – the part of the Integrated Management System, based on a business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security.
ISMS Manager	The individual responsible for managing and coordinating the ISMS. If the organization does not appoint a dedicated ISMS Manager, the responsibilities of the ISMS Manager role are assumed by the IMS Manager.
Information Security Risk	A risk whose impact implies a violation of information security.
Integrity	The property of safeguarding the accuracy and completeness of information and IT assets.

4 Information Security Management System

4.1 General

ISO/IEC 27001:2022 defines the ISMS as a part of an organisation's overall management system, based on a business risk approach. The company implements a central ISMS with strong decentralized responsibility and participation: each team and function is accountable for managing information security risks within their area of accountability.

In addition, the ISMS supports compliance with NIS2 by establishing governance for cybersecurity risk management and operational resilience, including defined roles and escalation paths, supplier risk oversight, incident management and reporting arrangements where applicable.

The company's ISMS addresses requirements defined in ISO/IEC 27001:2022, Clauses 4–10, and includes all applicable controls from Annex A. All applicable controls are documented in the Statement of Applicability (SoA).

The following must be adhered to when implementing and maintaining the ISMS:

- **Organisation:** Each team and function is responsible for managing information security risks and must implement effective organisational structures. Roles and responsibilities are defined in the **MOI Tech_IMS Scope**.
- **Information classification:** All teams and functions must identify and classify information requiring protection in accordance with the **MOI Tech_Information_Classification_Policy**.
- **Risk management:** Each team and function must establish an IS risk management process, including defining risk tolerance, identifying and assessing risks, making treatment decisions, monitoring risks, and communicating regularly with stakeholders.
- **Controls:** Control objectives and controls must be applied in order to comply with ISMS requirements. Controls may address baseline information security requirements or increased protection requirements identified through risk assessment.

- **Documentation:** All applied methodologies, processes, activities and major decisions regarding IS risk management must be documented and maintained.
- **Review and improvement:** The effectiveness of information security management must be reviewed at least annually. Reviews must cover IS organisation, objectives, completeness of risk coverage, and adequacy of risk measures.

In accordance with ISO/IEC 27001:2022 Amendment 1:2024, the Company considers climate change as a potentially relevant issue within the context of the ISMS. The ISMS Manager is responsible for assessing whether climate change poses a material risk to information security, in coordination with relevant business units and stakeholders.

4.2 ISMS Objectives

The information security objectives of **LLC MOI Tech, LLC MOVI TECH** are defined annually in the **MOI Tech_IMS Objectives_2026**.

4.3 Roles and Responsibilities

Role	Responsibilities
CEO	Approves the Information Security Policy and all major IS documents; provides necessary resources; ensures that the ISMS is aligned with business objectives.
ISMS Manager	Develops, implements and maintains the ISMS; coordinates information security risk assessments and treatment activities; manages the internal audit programme; reports to top management. If the organization does not appoint a dedicated ISMS Manager, the responsibilities of the ISMS Manager role are assumed by the IMS Manager.
IMS Committee	Reviews and approves significant changes to the IS; acts as a Change Advisory Board (CAB); reviews audit results; supports the implementation and improvement of the ISMS.
All personnel	Comply with all IS policies and procedures; report information security incidents; complete information security awareness training.

4.4 ISMS Implementation

After a major reorganisation, an ISMS implementation concept must be developed and approved within 12 months. An implementation plan must define responsibilities and milestones for each ISMS component in accordance with the **MOI Tech_Implementation_Order**.

All IS documents must be approved by the CEO and published and maintained in accordance with the **MOI Tech_Document_and_Records_Management_Procedure**.

Validity and Document Management

This Policy is effective as of **20.02.2026**. The **IMS Manager** is responsible for its maintenance and must conduct a formal review at least annually.

The effectiveness of this Policy is evaluated based on:

- **Compliance:** Alignment with applicable laws, regulations, and contractual obligations.
- **Awareness:** Level of personnel familiarity with their security roles and responsibilities.
- **Risk Context:** Continuous assessment of internal and external factors, including environmental and contextual risks, affecting information security.