02-ISMS Information Security Management System (ISMS) Policy

Purpose

This policy provides a framework to be applied when establishing, implementing, maintaining, and continually improving the information security management system ("ISMS"), as defined in *01-ISMS Scope of the ISMS*, in accordance with the requirements of the ISO/IEC 27001 ("ISO 27001") standard.

Leadership

Leadership and Commitment

The company is dedicated to establishing, implementing, maintaining, and continually improving the ISMS. Leadership commitment is demonstrated by the ISMS Governance Council when carrying out their responsibilities as defined in the *03-ISMS Roles, Responsibilities, and Authorities* document. The company will establish an information security policy and set information security objectives that are fully aligned with our strategic direction. The company will ensure that sufficient resources are available for the effective establishment, implementation, maintenance, and improvement of our ISMS. These resources will include:

- Financial support
- Skilled personnel
- Facilities and technical infrastructure

Information Security Policy

The company's top management establishes and upholds a dedicated information security policy. This policy:

1. Aligns with the organization's purpose and mission.
2. Incorporates our information security objectives or sets the groundwork for determining such objectives.
3. Demonstrates a commitment to meeting all relevant information security requirements.
4. Emphasizes our continual dedication to enhancing our information security management system.

For transparency and awareness:

1. This policy is documented and readily accessible.
2. It is actively communicated across all levels within The company.
3. Furthermore, we ensure this policy is available to relevant external parties, demonstrating our commitment to information security.

Roles, Responsibilities, and Authorities

The company has defined the roles, responsibilities, and authorities involved in establishing, implementing, maintaining, and continually improving the ISMS. The company has also defined how performance and competence will be measured and how competency gaps will be addressed. For further details, please refer to the *03-ISMS Roles, Responsibilities, and Authorities* document.

Planning

General Planning for the ISMS

The company prioritizes identifying key risks and opportunities, integrating solutions into our system, and continually monitoring and improving our approach.

Information Security Risk Assessment

Our consistent method for assessing risks ensures the identification of major security threats. We regularly evaluate and prioritize these risks and maintain documentation of all our findings. For further details, please refer to the *04-ISMS Risk Assessment and Risk Treatment Process* document.

Information Security Risk Treatment

The company is committed to selecting the right solutions for identified risks, implementing necessary security controls, and thoroughly documenting our choices while obtaining essential approvals. For further details, please refer to the *04-ISMS Risk Assessment and Risk Treatment Process* document.

Setting & Achieving Security Objectives

The company establishes clear, measurable security goals. We've developed a comprehensive plan detailing how to achieve them, allocating the needed resources and responsibilities, and continually monitoring our progress to make any necessary adjustments. Information security objectives are reviewed annually by the company's ISMS Governance Council based upon a clear understanding of business requirements. The current information security objectives are as follows:

1. Protect the confidentiality, availability, and integrity of company, customer, and employee data
2. Comply with applicable laws, regulations, and customer contractual obligations
3. Achieve and maintain ISO 27001 certification

Action plans to achieve these objectives are maintained and reviewed annually by the ISMS Governance Council. Refer to *10-ISMS Information Security Objectives Plan* for further details.

Planning Changes to the ISMS

When changes are deemed essential, The company ensures they are planned systematically, with careful consideration given to their potential impact on our overall security and the organization.

Support

Resources:

The company is committed to allocating the necessary resources to set up, execute, maintain, and consistently enhance our information security management system.

Competence:

1. We identify the expertise needed for roles impacting our information security performance.
2. Personnel are evaluated based on education, training, and experience to ensure they possess the required competence.
3. When necessary, the company will provide training, mentoring, or reassignment, or seek external expertise, while also maintaining evidence of such competencies.

Awareness:

1. All personnel are made aware of our information security policy and complete annual awareness training.

2. They understand their role in the success of the information security management system and the repercussions of non-compliance.

Communication:

1. The company identifies and acts on the need for both internal and external communications concerning our information security practices.
2. Decisions encompass what, when, how, and with whom to communicate.

Relevant information security policies will be communicated to all in-scope personnel at least annually after review and approval, or after any significant changes occur to the policy. The policy will be made available internally. For further details, please refer to the *06-ISMS Information Security Communication Plan* document.

Control of Documented Information

Documented Information:

Our system comprises information explicitly mandated and any other documentation we deem crucial for the effectiveness of our security measures.

Documentation creation and updates consider proper identification, format, and approval mechanisms.

To maintain the integrity of our documentation, we have protocols in place to control distribution, access, storage, changes, and preservation.

External documentation, deemed essential, is identified and managed effectively within our system.

The company has defined a procedure for the control and protection of documented information. For further details, please refer to the 05-ISMS Procedure for the Control of Documented Information document.

Operation

Operational Planning and Control

The company will plan, execute, and oversee the processes vital to satisfy the requirements and actions outlined in Clause 6. The company will maintain the necessary documented information. Planned modifications will be overseen, and the implications of unplanned changes will be evaluated. Appropriate actions will be taken to counteract any negative effects. Externally sourced processes, products, or services crucial to the information security management system will be governed by the company.

Information Security Risk Assessment

The company will conduct risk evaluations at scheduled intervals or in light of significant alterations, adhering to the criteria highlighted in 6.1.2 a). A record of the outcomes of these risk assessments will be preserved.

Information Security Risk Treatment

The company is committed to executing the information security risk treatment plan. For accountability, documented information on the outcomes of the risk treatment will be maintained.

Internal Audit

The company performs internal audits of its ISMS annually and has defined an ISMS Internal Audit Procedure. For further details, please refer to the *07-ISMS Procedure for Internal Audits* document.

Management Review

The company has defined an ISMS Management Review Procedure consisting of the necessary inputs and outputs to ensure that The company's ISMS is operating effectively, as intended, and is continually improving. For further details, please refer to the *08-ISMS Procedure for Management Review.*

Improvement

Continual Improvement

The company is dedicated to perpetually enhancing the relevance, sufficiency, and efficiency of our information security management system.

Nonconformity and corrective action

In case of any deviation from established standards, the company commits to:

- Address the nonconformity, manage its effects, and implement necessary corrections.
- Evaluate the root cause, ensuring it doesn't repeat or emerge in other areas.
- Act upon any required changes and validate the efficacy of those changes.
- All measures taken will be proportionate to the severity of the nonconformities identified.

For transparency and due diligence, the company will document:

- The specifics of any nonconformity and the corrective measures applied.
- The outcomes of those corrective actions.

The company has defined an ISMS Corrective Action and Continual Improvement Procedure when non-conformities are identified. Non-conformities may be identified during internal audits, external audits, management reviews, or ongoing monitoring of the ISMS. For further details, please refer to the *09-ISMS Procedure for Corrective Action and Continual Improvement* document.

Policy Violation

All company personnel (including employees, contractors, and applicable third parties) must maintain the security, confidentiality, availability, integrity, and privacy of company assets. Violations of ISMS policies and procedures may be considered serious breaches of trust, which can result in disciplinary action up to and including termination of employment or contract and prosecution by applicable federal, state, and local laws.

ISO 27001 Coverage

ISO 27001 4.1; 4.2; 4.3; 5.1

Document History

Version	Date	Description	Written by	Approved by
1.0.0	27-Nov-2025	Initial Version	Ryan Rich	Míra Stašek