Information Security Policy

1 Introduction

1.1 Scope

This policy sets out the company's requirements for the use of the Information Security Management System (ISMS), guided by the International Standard ISO27001:2013.

1.2 Revision History

Revision	Date	Record of Changes	Approved By
1.0	9/1/2024	Initial Issue	

1.3 Outline

The company's Information Security Management System (ISMS) complies with the requirements of the ISO 27001:2013 standard. With the present system, the Management team is committed to:

- the customer satisfaction
- the satisfaction of legal requirements
- the implementation and continuous improvement of the ISMS
- the continuous recognition of risks and opportunities
- the management of changes affecting the ISMS

The scope of the ISMS is:

«Legal Services»

In the context of the above commitment, the company has defined the following measurable quality objectives:

- to have the least possible non-conformities (system, services provided, etc.)
- to achieve the satisfaction of the requirements and needs of its customers.

The general and continuous objectives of our policy are the following:

- provide personalized advice and safe service to our customers.
- meet customers' needs and expectations.
- respect our customers for their dignity and privacy.
- ensure the immediacy and speed of customer/partner service.

To achieve the above objectives, the company applies an ISMS that complies with the requirements of the International Standard ISO 27001:2013. The objectives will be reviewed with the aim of continuous improvement of the system.

The Management team is committed to providing all the necessary material means and human resources to achieve its goals. All staff are obliged to follow the procedures and instructions resulting from the implementation of the ISMS.

1.4 References

Standard	Title	Description
ISO 27000:2014	Information security management systems	Overview and vocabulary
ISO 27001:2013	Information security management systems	Requirements
ISO 27002:2013	Information technology - security techniques	Code of practice for information security controls

1.5 Terms and Definitions

- "staff" includes all of those who work under our control, including employees, contractors, interns etc.
- "we" and "our" refer to company.

2 Policy Specifics

2.1 General

More specifically, the implemented information security policy is supported by:

- this general policy, which includes the objectives for the protection of information, the management's commitment to the implementation of the ISMS and the main principles and provisions of the security policy
- a series of individual policies aimed at defining detailed security policies in different areas of information security
- individual procedures and forms, where necessary, for the implementation of these policies

Information security is defined by the international literature as ensuring the following properties:

1. Confidentiality:

Access to information is allowed only to those who have appropriate authorization.

2. Integrity:

The information is complete, accurate and valid.

3. Availability:

The information is available at any time to an authorized user.

In addition to the above three main safety objectives, the following are considered complementary:

1. Identification and authentication of users:

The process of verifying the user's identity, i.e., ensuring that the user who is attempting to gain access is who he claims to be.

2. Access control:

Ensure that the user attempting to gain access is authorized.

3. Audit and monitoring:

Monitoring and recording of user actions.

4. Protection of personal data:

Protection of personal data and sensitive data of the individual from unauthorized collection, storage and processing.

5. Non-disclaimer:

Ensure that a user cannot deny that they have performed an action related to accessing or processing information, system and application.

The achievement of all the above security objectives, basic and complementary, leads to the maximum possible protection of information, systems and applications.
The Management team fully recognizes the objectives of the ISMS, supports their implementation in accordance with the present policy and ensures the continuous improvement of the system. More specifically, she is responsible for:

- the verification and approval of the initial version of the policy and any revision the policy
- the control and approval of roles and responsibilities related to the management of the ISMS
- monitoring significant changes in the organization or infrastructure of the company that create the need to revise the ISMS
- monitoring security-related incidents
- initiatives to strengthen information resources, in terms of security, by adopting additional measures.

3 Company Disclaimer

The company cooperated with a specialized consulting firm in the design and implementation of information security management systems, in accordance with the ISO 27001 standard and in the elaboration of consulting projects on information security issues.

4 Records

Records retained in support of this procedure are listed in the ISMS Controlled Records Register and controlled according to the Control of Management System Records Procedure.

On behalf of the Management Team

IOANNIS MARAKAKIS
17.01.2024 14:55