ELENIA'S INFORMATION SECURITY POLICY

The Information Security Policy is based on Elenia's strategies, values, Code of Conduct and the ISO/IEC 27001 standard. The aim of the policy is to define the goals, responsibilities and procedures of information security.

This policy applies to the information security management system, the scope of which is defined in the statement of the information security management system's field of application. The employees of Elenia Group companies and Elenia's partners comply with the guidelines defined in the policy.

1. Goals, management and responsibilities

The goal of information security is to ensure the confidentiality, integrity and availability of Elenia's information and data processing systems.

Elenia's IT principles, basic functions, continuity and information security principles are described in Elenia's IT policy. Responsibilities and governance are described in Elenia's cyber strategy. Our operations comply with the legislation, regulations and other statutes that govern information security and data protection.

The necessary procedures will be issued to support the principles and goals of the Information Security Policy. The procedures will describe the administrative and technical measures for protecting information and ensuring the continuity of operations in normal and exceptional conditions.

Information security work is integral to all work tasks and it is a continuous process to which everyone is committed in both their own work and as part of the business processes. All Elenia employees and partners must comply with this policy, procedures and contractual obligations in their operations, and are responsible for contributing to the information security of data under their control. The owner of certain data or a service has principal responsibility for the related information security.

The provider of the IT system or service is responsible for the information security of the service in question, compliance with information security requirements, and the continuous monitoring and development of information security. Every information processor is obligated to report, without delay, any deficiencies detected in information security and any suspected malpractice or infringements of information security in line with the instructions in force.

Elenia is committed to the continuous improvement of the information security management system and the assessment of its suitability, adequacy and effectiveness.

2. Information security concepts

Information security Maintaining the confidentiality, integrity and availability of information.

Information security management system (ISMS): An element of the management system, based on the assessment of business risks, to enable the creation, implementation, use, monitoring, auditing, maintenance and improvement of a high level of information security.

Confidentiality: The information and systems are accessible for authorised users only. Confidentiality is linked to the reliable verification of personal identity (authentication) and the legal non-repudiation of data usage.

Integrity: The information and systems are reliable, accurate and up-to-date, and have not been, or cannot be, modified in an uncontrolled manner as a consequence of hardware or software faults, natural events or human activity.

Availability: The information and services of the systems are available for use by authorised users within a pre-defined response time. The information has not been destroyed and cannot be destroyed as a consequence of faults, incidents or other activities.

3. Management methods

Information security maintenance and development are a continuous process that makes use of administrative, physical and IT solutions. We take information security into account in all the decisions we make.

An adequate and appropriate level of information security measures is ensured as part of the company's risk management, in compliance with the information security management system's risk management methodology. The measures necessary for remedying identified failures and reducing risks are documented in the risk register. The owners of the information and systems are responsible for performing corrective and preventive measures.

4. Performance indicators, monitoring and communications

Information security is ensured on the basis of continuous monitoring, performance indicators and reporting on security levels and information security events. Technical and administrative methods are used in monitoring. The information security manager coordinates the monitoring of information security and reports on the levels of information security, and information security events, to the management as part of the quarterly reporting process.

Performance indicators for information security:

1. Coverage of information security training
2. Fulfilment of contractual obligations in information security
3. Situation awareness of information security in information systems

Information security training is mandatory for all Elenia employees and partners using Elenia's information systems. Access rights to information systems can only be granted after passing the introduction to information security and data protection, and signing the information security agreement.

Fulfilment of information security obligations and partners' level of information security are monitored through in-house control and by using external evaluations and audits.

In order to ascertain statutory compliance and compliance of activities and to detect targets of improvement, the information security levels of the IT environment and information systems are assessed through in-house control and by using external evaluations and audits.

Information security communications are implemented in line with the annual information security calendar.

25.6.2019
Tapani Liuhala
CEO

ELENIA