31.3.2025

Elenia's Information Security Policy

Our mission
Electrifying life

Our vision
Responsible reformer of energy services and markets

Our values
Responsibility for the future | Close to the customer
Open and reliable cooperation | The courage to renew

Our strategic objectives are to earn our customers' trust, operate efficiently, renew the energy markets and services, enable the green transition, mitigate climate change and advance carbon neutrality. Our Code of Conduct and management system promote responsibility and sustainable development in everything we do.

Scope of application

The Information Security Management System and policy, based on the ISO 27001 standard, apply to the Elenia Group companies. This policy outlines the management's commitment to implementing information security at Elenia.

The scope of the Information Security Management System is described in the document "Elenia ISO/IEC 27001 Information Security Management System Scope". The Information Security Management System is reflected in our strategies, processes, and daily operations. The policy guidelines are followed by the personnel of Elenia Group companies and Elenia's partners.

According to our strategy, our goal is to achieve world-class information security. As part of responsible network development and the development of new products and services, we consider safety and the environment in all our decisions. We work to ensure that Elenia employees and our partners can work daily in a safe, healthy, and motivating environment.

Commitments

Elenia's principles and commitments to responsible management are described in Elenia's Sustainability Policy.

Objectives, management and responsibilities

We ensure the smooth running of our customers' daily lives, the societal resilience, and the continuity of operations in all situations. We prepare for the scarcity and reduced availability of natural resources. We continuously monitor and promote the safety of our electricity network.

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

Elenia's IT and information security principles and basic operations, along with up-to-date contact information, are described on Elenia's intranet site. Information security responsibilities are also described at a principle level in Elenia's Cyber Strategy (ID 115522).

Our operations comply with laws, regulations, and other requirements related to data protection and information security.

Appropriate procedural guidelines support the principles and objectives of the information security policy. The procedural guidelines describe administrative and technical measures to protect information and ensure the continuity of operations in normal and exceptional situations.

Information security work is included in every job and is a continuous process to which everyone is committed, both in their own work and as part of business processes. Every Elenia employee follows this policy and procedural guidelines in their activities. Elenia's partners comply with their contractual obligations and are responsible for the information security of the information under their control.

The person responsible for the information system or service provider is responsible for the information security of the system, compliance with information security requirements, and the continuous monitoring and development of information security.

Every information handler is obliged to immediately report any observed deficiencies in information security and suspected misuse or information security breaches in accordance with the current guidelines.

We are committed to continuously improving the Information Security Management System and assessing its suitability, adequacy, and effectiveness.

Information Security Concepts

Information Security: Ensuring the confidentiality, integrity, and availability of information.

Information Security Management System: A part of the management system based on business risk assessment, which is used to create, implement, operate, monitor, review, maintain, and improve good information security.

Confidentiality: Information and systems are only accessible to those authorized to use them. Confidentiality is tied to reliable identification (authentication) and the legal non-repudiation of information use.

Integrity: Information and systems are reliable, accurate, and up-to-date, and have not been altered or are not alterable in an uncontrolled manner due to hardware or software failures, natural events, or human actions.

Availability: Information and services are accessible to those authorized to use them within a predefined response time. Information is not destroyed or destructible due to failures, events, or other actions.

Control Measures

Maintaining and developing information security is a continuous process that uses administrative, physical, and technical solutions.

The appropriate and correct level of information security measures is ensured as part of the company's risk management according to the risk management methodology of the information security management system. Measures necessary to correct identified deficiencies and reduce risks are documented in the risk register. Responsible persons and service providers perform corrective and preventive measures.

Monitoring and follow-up

Ensuring information security involves continuous monitoring, measurement, and reporting of the security level and deviations. Monitoring is carried out using technical and administrative means. The Information Security Manager coordinates the monitoring of information security and reports the security level and deviations to the management.

The main indicators of information security are the number of information security incidents and the number of power outages caused by them during the year.

In accordance with Elenia's management system, it is possible to set other temporary or permanent indicators for business and operational purposes if they are considered to support the management and development of operations.

Information security training is mandatory for all Elenia employees and partners who use Elenia's information systems. Access to information systems can only be obtained after the successful completion of information security and data protection training and the signing of the information security commitment.

The level of information security in the IT environment and information systems is assessed through internal and external audits to determine compliance with laws and requirements, identify areas for improvement, and monitor the level of information security of partners and compliance with information security contractual obligations.

Information security is communicated according to the information security annual clock and when it is necessary to highlight a current issue.

Reference Documents

- ISO/IEC 27001 standard
- Statement of the scope of the Information Security Management System
- Information security risk management methodology
- Implementation plans for the Information Security Management System
- Sustainable development policy
- Laws, regulatory requirements, and standards

Elenia is Finland's second-largest distribution system operator and the largest customer service provider in the energy sector in Finland. We see to the maintenance and renewal of the electricity network, build electricity networks and connections together with our partner companies, measure our customers' electricity consumption and forward energy data to electricity suppliers. Our service business provides customer service as well as diverse services related to the electricity market for the energy sector and other infrastructure companies.

ELENIA