Grano's information security policy

Table of contents

Revision history

version	date	revised by and description
0.9	8 February 2021	PH, initial version submitted for commenting
0.9.1	8 March 2021	PH, AL. Revised based on comments
0.9.2	18 March 2021	Revised version by an external expert
0.9.3	18 March 2021	PH revised version
0.9.4	22 March 2021	PH revised versions, changes based on comments
1.0	25 March 2021	Board, first approved and published version
1.0.1	7 May 2021	Fixes for translation

Information security policy

Introduction

This information security policy is a strategic policy approved by the management of Grano Oy that defines Grano's key information security objectives, the methods for achieving them, the organisation of information security management and related responsibilities. In this policy, information security means ensuring the confidentiality, integrity and availability of all forms of information. Information security is also about compliance with applicable laws and regulations and the information security requirements imposed by cooperation partners. One of the aims of the policy to communicate that we consider information security matters to be important.

Grano manages and develops its information security in a risk-based manner using appropriate and cost-efficient solutions. The appropriateness of this information security policy is assessed annually by Grano's management team.

This information security policy together with Grano's values, risk management policy, security policy and data protection policy is an essential part of the corporate governance of Grano and Panostaja.

This information security policy and related clarifying instructions are published on Grano's intranet and apply to Grano's entire personnel and all areas of operation as well as all other persons who have been granted access to Grano's information.

This policy may be disclosed to stakeholders for the purpose of communicating about security matters in connection with the procurement and supply of services.

Goal

This policy defines the basic requirements for information security management and provides a basis for planning and implementing operations in compliance with the policy. To facilitate the practical implementation of the policy, Grano also maintains more detailed instructions focusing on specific areas of information security.

The information security policy expresses Grano's ambition, which is clarified with the policy's annexes and practical information security instructions. For external parties, such as subcontractors and service providers, the requirements of this policy are integrated into supply contracts where applicable.

The primary goal of information security management is to ensure the continuation of operations that Grano is responsible for in all circumstances. Appropriate and systematic information security management ensures the usability, data integrity and confidentiality of the ICT solutions linked to Grano's operations. This principle must be realised under all circumstances and in the context of all processes, registers and services. The information security policy provides the basis for ensuring the disruption-free operation and secure information processing of Grano's information systems.

At Grano, safeguarding customer data, the material supplied by customers and other data produced and processed by Grano's functions is an essential part of responsible operation.

Information security management model and responsibilities

Every person working at Grano is responsible for information security matters as part of their other duties in accordance with their own job description and areas of responsibility. This means that the personal responsibility to take care of information security matters cannot be transferred to others or outsourced.

Employees are responsible for familiarising themselves with the issued instructions and regulations concerning information security and complying with them. Furthermore, every employee is responsible for participating in assigned training and reporting any observed information security incidents, problems, threats and non-compliance with instructions to the Information Security Officer without delay.

The Information Security Officer develops and coordinates information security work at Grano and serves as the contact person for stakeholders in information security matters. The Information Security Officer manages the realisation of information security in accordance with this policy and associated instructions. The Information Security Officer reports on the state of information security once a year in writing.

Information Management coordinates Grano's information security management process and is responsible for associated reporting. Information Management identifies information security risks and defines measures for managing them in collaboration with Grano's business units and support functions.

The Board of Grano is responsible for assessing internal information security management and the effectiveness of risk management systems. In this role, the Board approves the group's information security policy, discusses Grano's key information security risks and the management thereof in its meetings and issues associated instructions, when necessary.

The President & CEO is responsible for ensuring that processes and polices related to information security are systematically managed as part of Grano's risk management system. The President & CEO is assisted with the implementation of information security by the company's information management and risk management functions.

External operators are responsible for familiarising themselves and complying with the regulations, orders and instructions concerning information security supplied to them and for informing their contact persons of any information security incidents, problems, threats and non-compliance with instructions related to Grano that they observe without delay.

Realisation of information security

Grano's information security management is steered by (1) Finnish and EU legislation concerning information security and data protection; (2) the key risks identified as part of information security management and risk management. Grano's information security management model is part of the group's risk and continuity management model.

Risk assessment

Risk assessment is carried out in accordance with the Board of Grano's policies. Individual risk assessments are conducted and the measures necessitated by them are monitored regularly by the Information Security Officer. They are also reported on at least once a year.

Information categorisation and processing

Grano employs an information categorisation method that includes instructions on how information should be categorised and defines information security controls for the processing of information belonging to different categories.

Processing of personal data

The ways in which customer and personal data are processed at Grano is defined in Grano's data protection policy and associated instructions.

Information security requirements

At Grano, information security requirements define the minimum level of information security that contract partners are required to adhere to.

Information security training

All Grano personnel are required to complete an annual online training unit on information security. The completion of the training unit is monitored. Select target groups are also provided with additional information security training relevant to their duties.

Management and monitoring of information systems

Maintaining and improving the level of information security require the systematic monitoring of the operation of information systems. The persons carrying out this monitoring are, by law, bound by professional secrecy as regards the information that they process as part of their work.

The state of information security is reported upon in connection with internal control and internal and external inspections. Technical information security is constantly assessed and separate information security inspections are conducted on the most important environments.

Processing of information security incidents

An information security incident means an incident that compromises one of the three basic elements of information security (confidentiality, integrity and availability). Grano has procedures and services in place for detecting information security incidents. The company also has defined procedures in place for processing potential personal data breaches, which are also reported to the management. Everyone who has been granted access to Grano's information is obliged to immediately report any observed information security incidents to the Information Security Officer or their designated contact person.

Information security violations

An information security violation is defined as an action that violates this information security policy and associated instructions. Grano has procedures in place for processing information security violations.

Communication

Grano's information security policy is public. Responsibilities related to information security are defined in greater detail in the policy's annexes, which are Grano's internal documents.

Information security matters, related orders and instructions and the changes thereto are communicated to Grano personnel via internal training and the company intranet. The party responsible for internal communication is Grano's Information Security Officer.

Compliance

Compliance with this information security policy and associated instructions is expected of everyone who processes information belonging to Grano. Compliance with this information security policy and associated instructions is mandatory. Violations and non-compliance can be used as grounds for a warning, termination of employment or criminal sanctions.