Granite

INFORMATION SECURITY POLICY

18th August 2021

Granite company level

ISO 27001 CERTIFIED BY

nixu

NIXU CERTIFICATION OY

1. Overview

One of the basic premises for Granite's operations is smooth and functional information management: the information should be available to those who need it, the accuracy of the information should be reliable, and access to certain information, such as corporate secrets, should be restricted. Granite's corporate secrets include e.g. information related to customer relations, R&D and strategic details.

Guaranteeing the smooth course of business operations and the customers' trust in Granite's ability to deliver the agreed-upon services require secure information processing, i.e. information security. When it is managed well, information security creates competitive edge and helps to achieve the aims set for business operations when the risks related to the data are under control. Looking after information security is a part of the duties of each Granite employee, regardless of their work tasks.

This information security policy outlines the aims, obligations and implementation methods that help manage the risks related to the data. A separate information security and privacy description is maintained for service production.

2. Definitions

Information security means protection of data, systems, services and telecommunication from administrative and technical procedures. Information security covers protection of data in electronic, verbal and written form. The purpose of the protection is to ensure the confidentiality, integrity and availability of the data:

- **Confidentiality**: the data is only available to the parties who are entitled to it.
- **Integrity**: the data is reliable, accurate and up-to-date.
- **Availability**: in terms of practical operations, the data can be used at the right time and without disruptions.

Risk refers to an event or factor potentially threatening the achievement of objectives. At Granite, risk refers to e.g. leaking the customers' confidential data or unplanned service downtime in service production.

3. Scope and objectives

This information security policy concerns all of Granite's operations, i.e. all the different areas of business and the whole personnel, including board members. This policy is observed in terms of applicable parts between Granite and its partners or other possible interest groups.

This policy conforms the European union's General data protection regulation (GDPR) and other best practices concerning privacy and data protection.

The aim is to make information security thinking a natural part of Granite's normal operations, in which case the information can be used whenever needed, the operations become smooth and possible risks can be anticipated in advance. This requires taking information security into consideration especially in R&D and service production. The customers' demands should be implemented as a part of Granite's total information security.

In addition, the aim is to maintain ISO27001 certified best practices of information security management, in which risks related to information security do not pose a threat to the continuity of the company's operations or its image or cause significant disruptions or costs to the company's operations.

4. Organization and responsibilities

Granite's Board of Directors is the highest party making decisions on information security. The Board of Directors will approve the information security policy and the amendments made to it.

The CEO is responsible for coordinating information security and may allocate responsibility for parts of the whole to other members of personnel or to a service provider. The Security Team described in the Risk Management Policy is responsible for handling all operative information security topics. In the case of information security incidents, guidelines described in the Business Continuity Plan will be followed.

Each employee is responsible for information security for their own part by operating in accordance with the training and guidelines provided. Each employee is responsible for reporting problems and deviations related to information security to the CEO or Security Team.

5. Implementation methods and principles

Information security controls and principles are based on the ISO27001 standard as Granite is certified accordingly. All the standard's 14 domains are implemented with selected controls:

- A.5 Information security policies
- A.6 Organization of information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operations security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance

Applicable controls are reviewed annually during the ISO27001 audits and internal audits. Additionally, the Security Team constantly monitors the status of the controls and their effectiveness.