INFORMATION SECURITY POLICY

14th April 2018

Granite corporate level

Granite

Kauppakatu 3 A
33200 Tampere
Finland

Vantaankoskentie 14
01670 Vantaa
Finland

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.

Information security can also be divided into operational areas in order to understand the whole. Information security is divided into eight areas:

- **Administrative security**: Management, determining responsibilities and resources and risk management.
- **Personnel security**: Personnel training and orientation.
- **Physical security**: Access control and protecting from fire, water damage and break-ins.
- **Document security**: Identification, classification, storage and backup of important data.
- **Communications security**: Firewalls, remote connections and encrypted telecommunication.
- **Hardware security**: Acquisition of devices, management of the lifespan and secure principles of use.
- **Usage security**: Access control for systems and administration of user licences.
- **Software security**: Virus protection, information security properties for software and updating software.

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 achieve the basic level of information security defined by the Finnish government, 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. Organisation and responsibilities

Granite's CEO is the highest party making decisions on information security. The CEO 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. The CEO is responsible for processing deviations related to information security and the necessary procedures.

The CTO is responsible for the information security for R&D and service production.

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 CTO.

5. Implementation methods and principles

Administrative security

- The personnel responsible for information security review annually the state of information security and its development needs in terms of their own operations. The development needs are reviewed and the CEO decides on the necessary development measures and their schedule.
- When needed, confidentiality and security agreements are signed with the cooperation partners. Also, other information security requirements may be included in the agreements.
- If needed, competence related to information security is acquired from cooperation partners, and individual solutions related to information security can be outsourced. Granite shall always be in charge of the whole.

Personnel security

- Information security training is organised regularly to the entire personnel. New employees are trained during their normal work orientation.
- Each employee will sign a separate confidentiality agreement as a part of his or her employment contract.
- In addition, the employees abide with the customers' instructions regarding information security when they operate on the customer's premises.
- The Finnish Police will conduct a security investigation for each new employee.

Physical security

- There is access control to Granite's office building.
- A list is kept for the keys to Granite's office premises, and only the CEO or CTO can grant a key to an employer.
- The customers are not allowed on R&D premises.

Document security

- The data is saved on discs with an automatic backup system.
- Access to the information is restricted based on the needs of each employee's work tasks.
- Customer-specific data is always processed in accordance with customer demands.
- Confidential physical data material is disposed of with a shredder.

Communications security

- Connections to Granite's information systems are implemented with encrypted methods requiring user IDs.
- External connections between Granite and its customers or cooperation partners are encrypted.
- Offices are checked that there's no hostile network devices in place.

Hardware security

- When acquiring new hardware, both information security requirements and the purpose of use of the hardware are taken into consideration.
- Workstations and server storage systems that are removed from use will be overwritten using trusted methods in order to ensure the confidentiality of the data.

Usage security

- A list is maintained for the systems that are in Granite's use and an administrator is appointed for each system. The administrators are responsible for granting user rights to their respective systems. The administrators provide, when needed, user support and operate as contact persons for the system suppliers.
- The principle of minimum rights is applied to granting user rights, in other words the employee will only be granted the kind of rights that they need for their work tasks.
- User access rights are removed when work tasks change or terminate.
- The user access rights for the systems are reviewed regularly in order to remove unnecessary rights.

Software security

- All workstations include anti-virus software that updates automatically.
- All workstations include their own firewall software.
- Information security updates for the workstations are automated.
- Server software and information security updates are regularly installed.