STERA'S DATA SECURITY POLICY

This policy describes the goals and the course of conduct for Stera Group's (later, "Stera") data security policy, as well as its responsibilities and
its organization.

For the purposes of this policy, data security means ensuring the confidentiality, integrity, and availability of information, regardless of how it is presented. This policy defines the basic requirements for data security and provides the basis for the planning and implementation of activities under the policy. More detailed guidance materials will also be developed to address the various areas of data security to support the implementation of this policy.

Data security will be implemented and developed in a risk-focused manner by using appropriate and cost-effective solutions. The appropriateness of the data security policy will be assessed annually by Stera Group's Data Administration Steering Team.

The data security policy, together with Stera's values, risk management, security and data security policies, are an integral part of good governance at Stera.

The goals of the data security policy

The primary goal of the data security policy is ensuring the continuity of the functions that Stera Group is responsible for, in all circumstances. Appropriate and effective data security ensures the availability of the ICT solutions related to Stera's operations, and the integrity and confidentiality of data used in processes and services under all circumstances in all operating countries. This policy forms the basis for ensuring the security of Stera Group's information systems and data processes.

At Stera, securing the data generated and processed by customer data and other digital activities is an essential part of the responsible conduct that both our customers and our partners expect from Stera. The increase in digitalization means that more and more legislation is created to regulate data security. Every Stera Group employee in every operating country must comply with the Group's data security policy, the principles and instructions that complement it, and applicable laws.

Implementing data security

Risk assessment

Data security risks are evaluated and analyzed regularly based on their effect on business operations. A risk assessment should also be carried out during the configuration phase of new systems as well as in the event of significant changes affecting the criticality of operations.

Data management classification

Stera has a data a management classification system, which defines the classification and business criticality of data and takes access rights into account.

Handling personal data

The data security policy and guidelines define how personal data is handled at Stera.

Data security requirements

Stera's data security requirements define the minimum required level of data security for co-contractors. The level of security compliance can be verified by audits where necessary.

Data security training

Stera uses various regular measures to improve employees' awareness of data security. These include e.g. online training, scam message simulations, and news on the intranet. Additionally, certain focus groups will be given targeted data security training. These trainings will be partly planned together with the HR Team. Future training plans will take the completion of employee skills matrices where necessary and information security into account.

Control and monitoring

Improving and maintaining the level of data security requires systematic and continuous automated monitoring of the operation of data systems. Persons carrying out controls are required by law to keep confidential the information they handle in the course of their work.

Data security situation reports are made in conjunction with normal internal security inspections as well as internal and external audits. The technical aspects of data security are continuously assessed, and separate security audits are carried out in key environments.

Procedure for data security anomalities

Stera has procedures and services in place to detect security breaches. Potential data security breaches are handled by Data Administration and reported to the Group Management Team.

Data security violations

A breach of data security is defined as an activity that does not comply with data security policies and guidelines.

Areas of responsibility and their organization

The data security policy is approved by the Stera Group Management Team.

The data security policy applies to all Stera companies' operations in all Group operating countries. Stera's personnel must comply with the policy. Stera Group companies and entities are responsible for implementing the policy and allocating the necessary resources within their own operations.

The CEO is responsible for ensuring that Stera includes effective data security as part of its risk management system. The CEO is assisted in the implementation of data security by the Group's Data Administration. The Data Administration handles and monitors the Group's data security risks and the implementation of risk management measures, and reports on these to the Group Management Team.

The members of the Group Management Team are responsible for the implementation of data security. Data Administration coordinates and develops information security processes, is responsible for practical implementation together with service providers, is responsible for reporting, and works with business and common operations to identify data security risks and to determine management measures. Each Stera employee must recognize data security risks connected to their own work or the Group at large, and react to them in an appropriate manner. The coverage and applicability of training will be monitored with the help of Stera's HR Team.

Data security policy governance

The governance mechanism for Stera's data security approach is the BCP operating model, with information security as a separate component. In accordance with its agenda, the Stera Group Management Team monitors and evaluates, among other things, the effectiveness of Stera's internal control, its internal auditing, and the BCP operating model. Together with Data Administration, the Group Management Team handles the most significant data security risks to the Group.

Entry into force

Approved by Stera Group Management Team, in Turku, on 12.12.2022.