riskrate

Data security in riskrate

Data security is a crucial part of the riskrate software development.

Data security includes servers' external and internal security, verification of data in the service, testing, and monitoring of hardware and software, personnel confidentiality obligations, user identification, and data encryption in transit and at rest.

Server data security

The riskrate production environment operates on servers only authorized persons can access. Maintaining our production servers is the responsibility of Google Cloud, which is stored in Hamina, Finland. Google Cloud is a global cloud computing service provider trusted by cloud industry leaders. Google Cloud provides a secure and uninterrupted environment for service production by riskrate.

The data center service includes a high-quality power supply with backup power, cabling, ventilation, a fire protection system, and physically secure facilities. Only authorized persons have access to the data center and development environment, which have separate access control systems.

User rights to databases and information systems are secured through company—and employee-specific access rights. Only the use of tested and approved software is permitted in database processing, and third-party management software is forbidden. The use of database traffic interfaces from external networks has been prevented.

Uninterrupted operation, safeguards, and control

All data is encrypted in transit and at rest.

Particular attention has been paid to uninterrupted operation and fault tolerance in a risk-ridden server environment. Daily backup copies of all riskrate databases and files are stored in a separate building.

Testing and monitoring

The operation of the firewall and other technology is tested regularly. Attempts to gain unauthorized access to the data network and its services are monitored actively.

In addition to hardware and systems, the program's log files and user-caused error situations are monitored and analyzed regularly.

We actively obtain information on risks to the information system through several channels. Based on this information, we can prepare for problems and eliminate them before they arise.

Professional competence and obligation to secrecy

Riskrate personnel involved in service production receive training in the areas specified according to their duties. All personnel working with confidential customer information have signed non-disclosure agreements.

User identification and rights

Users of riskrate software are authenticated using personal usernames and passwords for individual sessions. Data transfer between riskrate servers and users' computers is encrypted using HTTPS technology.

Users must not disclose their usernames or passwords to others. Riskrate never asks users to disclose their passwords or confidential information by e-mail or other means. Issues related to the use of riskrate are communicated through primary users and news items.