# Data security in riskrate

Data security is a crucial part of the riskrate software development. Data security includes the external and internal security of servers, verification of data in the service, the testing and monitoring of hardware and software, the confidentiality obligation of personnel, user identification and the encryption of data communications related to the software.

## Server data security

The riskte production environment operates on dedicated servers to which only authorised persons have access. The maintenance of our production servers is the responsibility of Amazon Web Services. Amazon Web Services is a leading cloud computing service provider globally trusted by cloud industry leaders. Amazon Web Services provides a secure and uninterrupted environment for service production by riskrate.

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

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

## Uninterrupted operation, safeguards and control

Particular attention has been paid to uninterrupted operation and fault tolerance in riskrate server environment. Backup copies of all riskrate databases and files are made daily in a separate fire area, and changing data is constantly replicated onto a backup server.

## Testing and monitoring

The operation of firewall and other technology is tested on a regular basis. Attempts to gain unauthorised access to the data network and its services are monitored actively.

riskrate software and its updates are tested in a separate testing environment before their actual launch. In addition to hardware and systems, the log files related to the program are monitored and analysed on a regular basis, as are error situations caused by users.

We actively obtain information through several channels on risks to the information system. On the basis of such information, we are able to prepare for any 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 personal usernames or passwords to others. riskrate never asks users to disclose their passwords or other confidential information by e-mail or other means. Issues related to the use of riskrate are communicated through main users and news items.