

Information processing plays a key role in fulfilling tasks at EOS KSI Inkasso Deutschland GmbH. All of the essential strategic and operative functions and tasks are significantly supported by information technology.

Any infringement of information security can reduce EOS KSI Inkasso Deutschland GmbH's efficiency or, in the worst case, even bring business processes to a complete halt. This would cause considerable material and immaterial damage to EOS KSI Inkasso Deutschland GmbH or third parties (customers, defaulting customers).

An integrated information security process was initiated to ensure the long-term protection of information security in the business processes, thereby preventing damage and maintaining the efficiency of EOS KSI Inkasso Deutschland GmbH. Formal confirmation will be given by an external office in 2011 when the security process is certified in accordance with ISO 27001 (information security management) as an enhancement of the existing quality management system. This will protect both business processes supported by IT as well as all of the information at EOS KSI Inkasso Deutschland GmbH and that of third parties against the internal and external hazards that always exist whenever information technology is used.

Furthermore, it will achieve the legal security required for everyone involved in these business processes or affected by them.

This will benefit EOS KSI Inkasso Deutschland GmbH's customers and default customers both directly and indirectly, as well as increasing confidence in EOS KSI Inkasso Deutschland GmbH's work.

Within the scope of their activities, all employees (management, executives and members of staff) at EOS KSI Inkasso Deutschland GmbH are responsible for information security and obliged to meet this challenge. They must fulfil the applicable laws (e.g. German penal code, Works Constitution Act, Commercial Code, Social Security Code, laws and regulations on data protection) and contractual regulations.

The responsibility for information security is taken by qualified personnel. The main responsibility will continue to lie with EOS KSI Inkasso Deutschland GmbH's top-level management, making it an important role model. Information security is of vital interest for EOS KSI Inkasso Deutschland GmbH and, therefore, an important strategic objective.

For this reason, the following measures affecting information security are hereby confirmed:

Building security

- The entire outer shell of all buildings has been secured against unauthorized access by means of an alarm system.
- Doors and gates to the buildings have been secured by means of security locks.
- There are electronically secured security areas within the buildings that can only be accessed by authorized persons (access rights will be allocated e.g. for server rooms, finance departments) by means of a transponder.
- Based on business and security requirements, standards for access control have been established and documented and will be checked regularly.
- Outside normal business hours, all buildings are monitored by an external mobile guard service.

Data and document security

- All documents and drawings will be recorded and controlled in accordance with the certified QM processes, 'Recording/controlling documents' and 'Recording/controlling drawings'. This means that they will be checked, approved and updated before being handed out and, depending on their contents, only provided for authorized persons.
- As far as possible, only electronic documents and drawings will be used, because they can be controlled more securely.
- Physical documents will also be stored in specially provided storage rooms or cupboards that can be locked.
- Unauthorized third parties will not be allowed to access rooms (documented access control).
- Electronic data will only be exchanged with third parties via secured, encoded data lines.
- All changes to electronic data will be checked systematically and can therefore be reproduced at any time.
- Supply lines for electricity and telecommunications that transport data or supply information systems have been protected against tapping and damage.
- All equipment that contains storage media will be checked before disposal to ensure that all sensitive data and licensed software has been deleted or securely wiped.
- Measures have been implemented for recognizing, preventing and restoring to protect against malware, and appropriate awareness has been raised among users.
- Formal regulations, procedures and measures exist to protect the exchange of information for all types of communication devices.

EDP systems

- The EDP systems are located in special server rooms (inner rooms without windows) that meet the most demanding standards for such rooms.
- Only selected persons can access these rooms. The right to access an EDP room has been regulated in writing.
- Backup copies of information and software will be made and tested regularly in accordance with the accepted backup method.
- Servers are protected by UPS/emergency power systems.
- The network will be administered and controlled appropriately to protect it from threats, maintain the security of the systems and applications in the network, and secure transferred information.
- Access to the system is protected by user IDs and graded passwords. All clients will be protected by passwords.
- Passwords must be changed at regular intervals.
- Virus scanners have been installed on all computer systems and will be updated on a daily basis.
- EOS KSI's network is protected against unauthorized access by means of a multi-level firewall.

- The hard drives on all laptops have been encoded and can only be operated by entering a password.
- In general, physical documents and other junk data will be destroyed by a commercial shredder company. This company will equip EOS KSI Inkasso Deutschland GmbH with document destruction containers that will be picked up regularly and leave empty containers in exchange. This procedure will be recorded in detail.
- Authorized personnel will control access to the clients.
- Access will only be possible to applications and data that are needed directly (Access Rules).
- The use of external media, software, etc., is strictly forbidden; this will be checked at regular intervals.
- Only the system administrators are allowed to install software; they require explicit approval to do so.
- All of the company's assets have been clearly identified; they will be maintained in an inventory of all of the company's important assets.
- The access rights of all employees, contractors and third-party users to information and information-processing facilities will be revoked if their employment contract, contract or agreement is terminated. They shall be adjusted accordingly if changes are made.

Data protection and personal security

- All of the members of staff have been instructed in accordance with the Federal German Data Protection Act [Bundesdatenschutzgesetz/BDSG] and signed a statement attesting to this. This statement is an integral part of their employment contract.
- All workflows fulfil the provisions of this Act.
- Security tasks and responsibility have been defined and documented in accordance with EOS KSI Inkasso Deutschland GmbH's principles of information security.

Regulations for members of staff:

- a. Special regulations on data protection apply when telephoning or sending telefaxes to external recipients.
- b. Employees must lock their computers when they leave their workplace.
- c. Passwords may not be passed on to others. If a third party learns of a password, a new password must be assigned without delay.
- d. The permissible use of information and the company's assets in connection with information-processing facilities has been regulated for each member of staff.
- e. The principle of a cleared desk applies for papers and removable media; the principle of a blank screen applies for information-processing facilities.