IS Policy (Guideline)

The processing of information has an important role in the business of our company. Information security (IS) is an elementary component of our service provision and means for us that we protect the protection goals of availability, integrity and confidentiality for our and our customers' information as well as in data protection - that of the data subjects - through the use of modern information and communication technologies and organizational solutions.

These protection goals are binding for all business activities in our company, all actions of employees and matters of the Information Security Management System (ISMS). Ensuring information security is the benchmark for all managers, employees as well as for all external employees, suppliers and service partners. The specifications of the ISMS are aligned with the organizational goals.

All decisions and actions in our company must be made taking into account operational and economic aspects and taking into account the requirements of information security in order to guarantee an effective level of information security. In addition, compliance with and implementation of laws, regulations and contractual obligations is an equivalent principle of action. To ensure this, we have set up a process to determine these requirements. Where necessary, further guidelines are laid down to ensure and regulate information security.

For this purpose, we have defined, implemented, carried out, monitored, reviewed, maintained and continuously improved an information security management system (ISMS). The management has defined an organizational structure in the form of an information security officer (ISO) and necessary supplementary roles. This ensures the embedding of information security in business processes. Internal and external values shall be determined, classified and managed. Threats and vulnerabilities that threaten the information security of the values must be analyzed. Risks must be identified and treated on the basis of an IS risk process and defined risk criteria and minimized by means of risk countermeasures. All employees are obliged to identify risks within the scope of their tasks and to report them to the immediate manager or the ISO.

Access to sensitive (classified) information is secured by means of a security concept for the organization and IT infrastructure at the site. Risk countermeasures are implemented after approval by the risk owner or the management in accordance with legal, contractual and internal regulations.

Through appropriate training and awareness-raising measures on information security as well as corresponding regulations such as guidelines and procedures, the awareness of information security among employees must be continuously maintained and further developed.

Information security breaches can have a significant negative impact on our business. For this reason, intentional and grossly negligent acts - which cause an information security breach - are to be expected to result in legal consequences. A disciplinary procedure has been set up for this purpose.

It is a joint task and duty of managers and employees (internal and external) to ensure information security. Every single employee - regardless of his or her position in our company and his or her area of responsibility - bears joint responsibility for ensuring information security in his or her working environment. It is expected that each employee will take action independently in the event of a detected information security incident. For this purpose, an information security incident process must be set up. In the event of an emergency, appropriate processes and emergency plans must be created and tested as part of Business Continuity Management (BCM).

This IS policy gives all employees of our company the clear mandate of the management to observe and implement all existing and future requirements for achieving the safety goals. It is subject to a document management process. Updates will be communicated to each recipient. If necessary, it will also be made available to external third parties.

In addition, information security is a basis of business policy and makes an indispensable contribution to the success of our corporate services. It was coordinated with the corporate strategy.

Our company is committed to continuously improving information security. For this purpose, information security objectives for all levels and functions must be defined, measured and improved in accordance with the above specifications.

The Management Board

originally signed by the CEO