Information Security Guideline

The management hereby adopts the following Information Security Guideline as part of their strategy:

Importance of Information Processing

Information processing plays a key role for our business operations. All essential strategic and operational functions and tasks are substantially supported by information and communication technology (ICT). We must be able to compensate a failure of the ICT systems in the short term. A collapse of our business, even in sub-areas, is not acceptable. Since our core competence lies in the partnership-based development of innovative devices in cooperation with customers and suppliers, the protection of this information from unauthorized access and modification is of vital importance.

Superordinate Goals

Our data and our ICT systems in all technology-dependent and commercial areas are safeguarded with regard to their *availability* so that expected downtimes will be acceptable. Failures and irregularities in data and ICT systems are only acceptable to a limited extent and only in exceptional cases (*integrity*). The requirements with regard to confidentiality are at a normal level and comply with the statutory requirements. Maximum confidentiality requirements apply with regard to the design data of our clients and in the development department.

The standard security measures must be in a financially justifiable proportion to the value of the protectable information and ICT systems. Damage events with a high financial impact must be prevented.

All employees of the company comply with the relevant laws (e.g. Data protection laws and regulations), internal procedural and work instructions and contractual provisions. Negative financial and non-monetary consequences for the company as well as for the employees due to violations of the law and breaches of contractual provisions are to be avoided.

All employees and the management of the company are aware of their responsibility in dealing with the ICT systems and support the security strategy to the best of their ability.

Detailed Objectives

Delayed or incorrect management decisions can have far-reaching consequences. Therefore, the management is dependent on current operational data

when taking major decisions. This information requires a high level of security in terms of availability and integrity.

Data protection law and the interests of our employees require ensuring that personal data concerning our employees are kept confidential. The HR department's data and ICT applications are therefore subject to a high level of confidentiality. The same applies to the data of our business partners.

Request and quotation information received from/submitted to our clients as well as design data from our customers and our development department are subject to very strict confidentiality requirements. Their loss or theft may result in competitive disadvantages or claims for damages against us. Confidentiality is protected and tampering prevented through technical measures and the attentiveness of our employees.

Systems availability and freedom from errors is ensured with regard to our logistics areas and production plants. Downtimes are acceptable only to a very limited extent, as these can directly or indirectly result in loss of income and negatively impact customer satisfaction.

The use of the Internet and of portal applications for obtaining information and for communication is a matter of course for us. E-mail replaces or supplements other office communication channels. Adequate measures ensure that the risks of use remain as low as possible.

Information Security Management

A security organization was established to achieve our information security goals. An Information Security Officer was appointed. The Information Security Officer reports directly to the management.

The Information Security Officer is provided with sufficient financial and time resources by the management to regularly participate in further education and information events and to reach the information security goals defined by the management.

ICT users shall support the ICT Security Administrators and the Information Security Officer in their tasks.

The Information Security Officer must be involved in all projects at an early stage in order to take account of security-relevant aspects at the planning stage. If personal data are affected, the same shall apply to the Data Protection Officer.

ICT users have to follow to the instructions of the Information Security Officer in security-related matters.

Security Measures

A person is appointed who is responsible for all procedures, ICT applications and ICT systems and determines the relevant protection requirements and access authorizations.

Substitutes shall be appointed for all functions with responsibilities. It shall be ensured through instruction and sufficient documentation that the substitutes will be able to perform their duties.

Buildings and premises are protected by adequate access controls. Access to ICT systems is protected by appropriate access controls and access to data through a restrictive authorization concept.

Computer virus protection programs are run on all ICT systems. All Internet access is secured by adequate firewall systems. All protection programs are configured and administered in such a way that they provide effective protection and prevent manipulation. Furthermore, ICT users shall support these safety measures through a safety-conscious working method and, in the event of abnormalities, information of the defined points of contact.

Data loss can never be ruled out completely. Comprehensive data backup therefore ensures that ICT operations can be resumed in the short term if parts of the operational database are lost or obviously faulty. Information is uniformly identified and stored so that it can be retrieved quickly.

In order to limit or prevent major damage as a result of emergencies, security incidents must be dealt with swiftly and systematically. Emergency measures are put together in a separate emergency precaution concept. Our goal is to maintain critical business processes even in the event of a system failure, and to restore the availability of failed systems within an acceptable period of time.

If ICT services are outsourced to external parties, specific security requirements are stipulated in the service level agreements. Insofar as data with high protection requirements must be made available to suppliers for the purpose of executing the contract, these suppliers will be separately and expressly obliged to observe secrecy by us. The right of oversight is defined.

ICT users participate in training sessions on the correct use of ICT services and related security measures. The management supports needs-based training and further education.

Improving Security

The information security management system is regularly checked for up-to-datedness and effectiveness. In addition, the measures are also regularly reviewed to determine whether the affected employees are aware of them, and whether they can be implemented and integrated into the operating procedure.

The management supports the ongoing improvement of the security level. Employees are encouraged to communicate possible improvements or weaknesses to the relevant points of contact.

The desired level of security and data protection is ensured through an ongoing review of the relevant rules and regulations and compliance with them. Deviations are analysed with the aim of improving security and constantly updating it in line with state-of-the-art ICT security technology.

Bamberg, 02/05/2018

- Management -

Thomas Mai

Stefan Frey

- Information Security Officer –

Ralf Ruf