People.Health.Care.

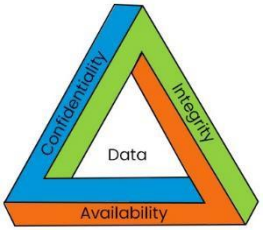
Information Security Policy

1 Company and business purpose, importance of information security

Lohmann & Rauscher (L&R) is a leading international company specializing in the development, production and distribution of medical and hygienic products. The company offers a wide range of products for wound care, orthopedics, compression therapy and care. These include bandages, medical compression stockings, orthoses and bandages, as well as surgical drapes and products for professional wound cleaning and care.
L&R's business purpose is to provide high-quality and innovative products and solutions for patients, healthcare professionals and caregivers to improve and facilitate patient care and healing.
L&R is therefore dependent on secure processes in the company. In this situation, it is essential to ensure information security in order to create the necessary reliability in everyday business.
L&R understands and commits to protecting information security as an essential customer service that protects the confidentiality and integrity of information and ensures the availability of our processes.
An active security culture is practiced in the company and information security is promoted by involving all employees, training them and raising their awareness. The employee is at the center of the active safety culture.

2 Purpose, Scope and User

The objective of this guideline, which is positioned at the highest level, is to define the purpose, orientation, foundations and basic rules for the information security management system (ISMS).
The scope of application of the ISMS covers all spatial, personnel, material and IT infrastructure components and values as well as processes and departments of L&R. Information security management applies to all L&R employees, initially in all of the company's locations in Germany and Austria, but is to be increasingly extended to all other L&R locations and associated companies worldwide. Employees and, if necessary, partners and suppliers are informed via relevant changes in this guideline, as well as other applicable regulations in the context of the ISMS.



3 Information Security Basic

Concepts Confidentiality

Confidentiality is the protection against unauthorized disclosure of information. Confidential data and information may only be accessible to authorised persons in the permitted manner.

Integrity

Integrity refers to ensuring the correctness (integrity) of data and the correct functioning of systems. When the term integrity is applied to "data," it expresses that the data is complete and unaltered.

Availability

The availability of services, functions of an IT system, IT applications or IT networks or even information is present if these can always be used by the users as intended.

Information Security

Maintaining the confidentiality, integrity, and availability of information means information security.

Information Security Management System

This is the part of the company's overall management process that deals with planning, implementing, maintaining, reviewing and improving information security in the company.

4 Information Security Management

4.1 Structure of information security

The starting point for the information security management system is the ISO 27001 standard.

The structure of the information security management system is shaped by the guideline and the guidelines derived from it in the company. Information security is implemented through the measures and processes derived from it, the associated documentation in the form of protocols, checklists, risk analyses and the passing on of information to employees, suppliers and customers.

The starting point for our ISMS is also the requirements of our interested parties/stakeholders. These are decidedly recorded in an overview.

4.2 Segregation of duties

In order to maintain the separation of duties in the company, operational tasks are separated from controlling tasks. In the course of this, care is taken to ensure that functions and roles are not performed by one person at the same time. such as rights management and review, network administration and auditing, etc. This approach is intended to ensure that the organization's security goals are met and not manipulated.

4.3 Targets and measurement

The general objectives of the information security management system are:

- Protection of the confidentiality, availability and integrity of information assets.
- A reduction in the damage caused by potential incidents
- Ensuring legal capability at all times
- Maximum protection of customer data, internal company data and personal data processed within the company.

These goals align with the company's business goals, strategy, and business plans. An important function in this context is covered by the role of an information security officer (FIT) in the company. This is responsible for reviewing the general ISMS targets and defining new targets.

Action objectives for individual security measures or groups of security measures are proposed by the information security officer and forwarded by OIS as an operational unit to the management for decision.

All these targets must be reviewed at least once a year.

L&R evaluates and measures the fulfilment of these targets. The ISB is responsible for defining the methodology used to measure the fulfilment of these targets. The assessment/measurement is carried out at least once a year. The FITR analyses and evaluates the measurement results and submits the report to OIS for subsequent forwarding to the management.

4.4 Information security requirements

All policies and the entire ISMS must comply with both legal and regulatory requirements as well as contractual obligations that are relevant to the organization in the field of information security.

L&R is committed to establishing, implementing, maintaining and continuously improving an ISMS in accordance with ISO 27001 regulations.

4.5 Asset and risk management

The essential cornerstone of the ISMS is asset and risk management. All information values relevant to the ISMS (primary assets), information carriers (secondary assets) and other relevant components for the ISMS are recorded and assigned to owners. All assets are subjected to a protection needs analysis, in which the 3 protection goals of information security are taken into account (see Chapter 3). Assets in need of protection are then subjected to a risk analysis. Further details are defined in the guidelines on asset and risk management.

4.6 Continuous improvement

Continuous improvement is ensured by the following measures:

- the ISMS is regularly reviewed for topicality and effectiveness. This includes regular audits and the effectiveness of measures.
- All employees are obliged to support the FITR in this task.

- Particular emphasis is placed on the use of technically up-to-date measures.
- The management of the company promotes the ISMS in the company.
- Deviations are analysed in detail and necessary measures are derived and implemented as improvements.
- All employees are involved in the ISMS to such an extent that they can report errors or improvement measures. This behavior is encouraged.
- Suppliers and service providers are sufficiently integrated into the ISMS and are regularly reviewed so that vulnerabilities can be identified and remedied.

4.7 Responsibilities

The following are the basic responsibilities for the ISMS:

- The management is responsible for ensuring that the ISMS is implemented and maintained in accordance with this guideline and that all necessary resources are available.
- The ISB is responsible for coordinating the operation of the ISMS, as well as for reporting on its performance.
- The management must review the ISMS at least once a year as part of a management review (or always in the case of significant changes). The purpose of this management review is to demonstrate the adequacy, suitability and effectiveness of the ISMS. The management review is prepared accordingly by the FIT, as part of the role of the FIT.
- The ISB is responsible for the implementation of information security training and awareness programs for employees.

- The protection of the assets is the responsibility of the owner of the respective information assets.
- Any security incidents or vulnerabilities must be reported to the ISB.
- The ISB defines which information related to information security is communicated with which interested parties (both internal and external), by whom and when.
- The FITR is responsible for setting up and implementing the training and awareness plan that governs all individuals who have a role in information security management.
- Employees and relevant external parties are informed of any innovations or changes affecting the ISMS and, if necessary, trained.
- Regular meetings for reporting to the management and exchanging information on the current status of information security at L&R will take place at least once a year.

4.8 Guideline Communication

The ISB ensures that all L&R employees, as well as - if necessary - other stakeholders are familiar with this guideline.

4.9 Consequences of non-compliance

The intentional or grossly negligent violation of ISMS guidelines can lead to sanctions. In the event of violations, disciplinary measures, in serious cases the termination of the employment relationship and legal action may be taken by the company.

5 Support for ISMS implementation

The management hereby expressly declares the relevance of information security at L&R and calls for the implementation of ISMS and its continuous improvement. At the same time, L&R will support this process with suitable resources in order to meet all the targets set out in this guideline and to maintain them in the future.

Yours sincerely,

The Executive Board

Rengsdorf / Vienna, April 2026

Thomas Menitz	Holger Mägdefrau	Fabio Cortesi	Dr. Klemens Schulz
CEO & COO	CFO	CCO	CPO