People.Health.Care.

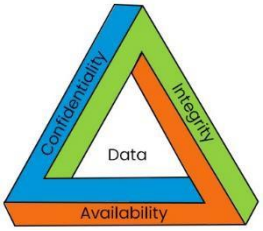
Richtlinie zur Informationssicherheit

1. Unternehmenszweck und Bedeutung der Informationssicherheit

Lohmann & Rauscher (L&R) ist ein führendes internationales Unternehmen, das sich auf die Entwicklung, Produktion und den Vertrieb von medizinischen und hygienischen Produkten spezialisiert hat. Das Unternehmen bietet ein breites Spektrum an Produkten für die Wundversorgung, Orthopädie, Kompressionstherapie und Pflege an. Dazu gehören Verbände, medizinische Kompressionsstrümpfe, Orthesen und Bandagen sowie Operationsabdeckungen und Produkte für die professionelle Wundreinigung und -pflege.
Der Unternehmenszweck von L&R besteht darin, hochwertige und innovative Produkte und Lösungen für Patienten, medizinisches Fachpersonal und Pflegekräfte bereitzustellen, um die Patientenversorgung und Heilung zu verbessern und zu erleichtern.
L&R ist daher auf sichere Prozesse im Unternehmen angewiesen. In diesem Kontext ist es unerlässlich, die Informationssicherheit zu gewährleisten, um die notwendige Zuverlässigkeit im Arbeitsalltag zu schaffen.
L&R versteht und verpflichtet sich, die Informationssicherheit als wesentlichen Kundenservice zu schützen, der die Vertraulichkeit und Integrität von Informationen sichert und die Verfügbarkeit unserer Prozesse garantiert.
Im Unternehmen wird eine aktive Sicherheitskultur gelebt, und die Informationssicherheit wird durch die Einbindung aller Mitarbeitenden, deren Schulung und Sensibilisierung gefördert. Der Mitarbeitende steht dabei im Mittelpunkt der aktiven Sicherheitskultur.

2. Zweck, Geltungsbereich und Nutzer

Ziel dieser Richtlinie, die auf der höchsten Ebene angesiedelt ist, ist es, den Zweck, die Ausrichtung, die Grundlagen und die Grundregeln für das Informationssicherheitsmanagementsystem (ISMS) festzulegen.
Der Anwendungsbereich des ISMS umfasst alle räumlichen, personellen, materiellen und IT-Infrastrukturkomponenten sowie Werte, Prozesse und Abteilungen von L&R. Das Informationssicherheitsmanagement gilt für alle Mitarbeitenden von L&R, zunächst an allen Standorten des Unternehmens in Deutschland und Österreich, soll jedoch schrittweise auf alle weiteren L&R-Standorte und verbundenen Unternehmen weltweit ausgeweitet werden.
Mitarbeitende sowie gegebenenfalls Partner und Lieferanten werden über relevante Änderungen dieser Richtlinie sowie andere anwendbare Regelungen im Kontext des ISMS informiert.



3. Grundlagen der Informationssicherheit

Konzepte Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Offenlegung von Informationen. Vertrauliche Daten und Informationen dürfen nur autorisierten Personen auf zulässige Weise zugänglich sein.

Integrität

Integrität bezieht sich auf die Sicherstellung der Richtigkeit (Unversehrtheit) von Daten und die korrekte Funktion von Systemen. Wird der Begriff Integrität auf „Daten“ angewendet, bedeutet dies, dass die Daten vollständig und unverändert sind.

Verfügbarkeit

Die Verfügbarkeit von Diensten, Funktionen eines IT-Systems, IT-Anwendungen, IT-Netzwerken oder auch Informationen liegt vor, wenn diese jederzeit wie vorgesehen von den Nutzern genutzt werden können.

Informationssicherheit

Die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen bedeutet Informationssicherheit.

Informationssicherheitsmanagementsystem (ISMS)

Das ISMS ist der Teil des gesamten Managementprozesses eines Unternehmens, der sich mit der Planung, Implementierung, Aufrechterhaltung, Überprüfung und Verbesserung der Informationssicherheit im Unternehmen befasst.

4. Informationssicherheitsmanagement

4.1 Struktur der Informationssicherheit

Ausgangspunkt für das Informationssicherheitsmanagementsystem ist der Standard ISO 27001.

Die Struktur des Informationssicherheitsmanagementsystems wird durch die Richtlinie und die daraus im Unternehmen abgeleiteten Leitlinien geprägt. Die Informationssicherheit wird durch die daraus resultierenden Maßnahmen und Prozesse umgesetzt, die dazugehörige Dokumentation in Form von Protokollen, Checklisten, Risikoanalysen sowie durch die Weitergabe von Informationen an Mitarbeitende, Lieferanten und Kunden.

Ein weiterer Ausgangspunkt für unser ISMS sind die Anforderungen unserer interessierten Parteien/Stakeholder. Diese werden in einer Übersicht systematisch erfasst.

4.2 Trennung von Aufgaben

Um die Trennung von Aufgaben im Unternehmen sicherzustellen, werden operative Tätigkeiten von Kontrollaufgaben getrennt. Dabei wird darauf geachtet, dass Funktionen und Rollen nicht gleichzeitig von einer Person ausgeübt werden, wie zum Beispiel Rechteverwaltung und Überprüfung, Netzwerkadministration und Auditierung usw.
Dieser Ansatz soll gewährleisten, dass die Sicherheitsziele der Organisation erreicht werden und nicht manipuliert werden können.

4.3 Ziele und Messung

Die allgemeinen Ziele des Informationssicherheitsmanagementsystems sind:

- Schutz der Vertraulichkeit, Verfügbarkeit und Integrität von Informationswerten.
- Reduzierung von Schäden durch potenzielle Vorfälle.
- Sicherstellung der rechtlichen Handlungsfähigkeit zu jeder Zeit.
- Maximaler Schutz von Kundendaten, internen Unternehmensdaten und personenbezogenen Daten, die innerhalb des Unternehmens verarbeitet werden.

Diese Ziele stehen im Einklang mit den Unternehmenszielen, der Unternehmensstrategie und den Geschäftsplänen. Eine wichtige Rolle in diesem Zusammenhang übernimmt die Funktion eines Informationssicherheitsbeauftragten (ISB) im Unternehmen. Dieser ist verantwortlich für die Überprüfung der allgemeinen ISMS-Ziele und die Definition neuer Ziele.

Handlungsziele für einzelne oder gruppierte Sicherheitsmaßnahmen werden vom Informationssicherheitsbeauftragten vorgeschlagen und von der Organisationseinheit OIS als operative Einheit der Geschäftsleitung zur Entscheidung vorgelegt.

Alle diese Ziele müssen mindestens einmal jährlich überprüft werden.

L&R bewertet und misst die Erreichung dieser Ziele. Der ISB ist für die Festlegung der Methodik zur Messung der Zielerreichung verantwortlich. Die Bewertung/Messung erfolgt mindestens einmal jährlich. Der FITR analysiert und bewertet die Messergebnisse und übermittelt den Bericht an die OIS, welche diesen anschließend an die Geschäftsleitung weiterleitet.

4.4 Anforderungen an die Informationssicherheit

Alle Richtlinien und das gesamte ISMS müssen sowohl den gesetzlichen und regulatorischen Anforderungen als auch den vertraglichen Verpflichtungen entsprechen, die für die Organisation im Bereich der Informationssicherheit relevant sind.

L&R verpflichtet sich, ein ISMS gemäß den Vorgaben der ISO 27001 aufzubauen, umzusetzen, aufrechtzuerhalten und kontinuierlich zu verbessern.

4.5 Werte- und Risikomanagement

Der wesentliche Grundpfeiler des ISMS ist das Werte- und Risikomanagement. Alle für das ISMS relevanten Informationswerte (primäre Werte), Informationsträger (sekundäre Werte) und andere relevante Komponenten für das ISMS werden erfasst und Eigentümern zugewiesen. Alle Werte werden einer Schutzbedarfsanalyse unterzogen, bei der die drei Schutzziele der Informationssicherheit (siehe Kapitel 3) berücksichtigt werden. Anschließend werden schutzbedürftige Werte einer Risikoanalyse unterzogen. Weitere Details sind in den Richtlinien zum Werte- und Risikomanagement definiert.

4.6 Kontinuierliche Verbesserung

Die kontinuierliche Verbesserung wird durch folgende Maßnahmen sichergestellt:

- Das ISMS wird regelmäßig auf Aktualität und Wirksamkeit überprüft. Dazu gehören regelmäßige Audits und die Überprüfung der Effektivität der Maßnahmen.
- Alle Mitarbeitenden sind verpflichtet, den FITR bei dieser Aufgabe zu unterstützen.
- Es wird besonderer Wert auf den Einsatz technisch aktueller Maßnahmen gelegt.
- Die Unternehmensleitung fördert das ISMS innerhalb des Unternehmens.
- Abweichungen werden detailliert analysiert und notwendige Maßnahmen werden abgeleitet und als Verbesserungen umgesetzt.
- Alle Mitarbeitenden werden in das ISMS in dem Maße eingebunden, dass sie Fehler oder Verbesserungsvorschläge melden können. Dieses Verhalten wird gefördert.
- Lieferanten und Dienstleister werden ausreichend in das ISMS integriert und regelmäßig überprüft, damit Schwachstellen erkannt und behoben werden können.

4.7 Verantwortlichkeiten

Die grundlegenden Verantwortlichkeiten für das ISMS sind wie folgt festgelegt:

- **Die Geschäftsleitung** ist dafür verantwortlich, dass das ISMS gemäß dieser Richtlinie implementiert und aufrechterhalten wird und dass alle notwendigen Ressourcen zur Verfügung stehen.
- **Der ISB (Informationssicherheitsbeauftragte)** ist für die Koordination des Betriebs des ISMS sowie für die Berichterstattung über dessen Leistung verantwortlich.
- **Die Geschäftsleitung** muss das ISMS mindestens einmal jährlich im Rahmen eines Management-Reviews (oder bei wesentlichen Änderungen) überprüfen. Ziel dieses Management-Reviews ist es, die Angemessenheit, Eignung und Wirksamkeit des ISMS nachzuweisen. Das Management-Review wird entsprechend vom FIT vorbereitet, im Rahmen seiner Rolle als FIT.

- **Der ISB** ist für die Durchführung von Schulungen und Sensibilisierungsprogrammen zur Informationssicherheit für Mitarbeiter verantwortlich.
- **Der Schutz der Werte** liegt in der Verantwortung der jeweiligen Eigentümer der Informationswerte.
- **Alle Sicherheitsvorfälle oder Schwachstellen** müssen dem ISB gemeldet werden.
- **Der ISB** legt fest, welche Informationen im Zusammenhang mit der Informationssicherheit mit welchen interessierten Parteien (intern und extern), von wem und wann kommuniziert werden.
- **Der FITR** ist verantwortlich für die Erstellung und Umsetzung des Schulungs- und Sensibilisierungsplans, der alle Personen umfasst, die eine Rolle im Informationssicherheitsmanagement innehaben.
- **Mitarbeiter und relevante externe Parteien** werden über Neuerungen oder Änderungen, die das ISMS betreffen, informiert und bei Bedarf geschult.
- **Regelmäßige Meetings** zur Berichterstattung an die Geschäftsleitung und zum Austausch von Informationen über den aktuellen Stand der Informationssicherheit bei L&R finden mindestens einmal jährlich statt

4.8 Richtlinie Kommunikation

Der ISB stellt sicher, dass alle L&R-Mitarbeitenden sowie – falls erforderlich – andere Stakeholder mit dieser Richtlinie vertraut sind.

4.9 Konsequenzen bei Nichteinhaltung

Die vorsätzliche oder grob fahrlässige Verletzung der ISMS-Richtlinien kann zu Sanktionen führen. Im Falle von Verstößen können disziplinarische Maßnahmen ergriffen werden, in schweren Fällen auch die Beendigung des Arbeitsverhältnisses sowie rechtliche Schritte durch das Unternehmen.

5 Unterstützung bei der Umsetzung des ISMS

Die Geschäftsleitung erklärt hiermit ausdrücklich die Relevanz der Informationssicherheit bei L&R und fordert die Umsetzung des ISMS sowie dessen kontinuierliche Verbesserung. Gleichzeitig wird L&R diesen Prozess mit geeigneten Ressourcen unterstützen, um alle in dieser Richtlinie festgelegten Ziele zu erreichen und auch in Zukunft aufrechtzuerhalten.

People.Health.Care.

Mit freundlichen Grüßen,

Der Vorstand

Rengsdorf / Wien, April 2026

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