FORTSCHRITT DURCH LEICHTIGKEIT.

# INFORMATIONSSICHERHEITS LEITLINIE

LEIBER GROUP GMBH & CO. KG
LEIBER POLAND GMBH

## Inhalt



### Änderungshistorie

| Version | Datum | Autor | Änderungen / Bemerkungen |
|---|---|---|---|
| 0.9 | 04.04.2025 | Hartmut Grande | Entwurf auf Basis ISO 27001:2022 / VDA-ISA 6.x |
| 1.0 | 31.07.2025 | Udo Faulhaber | Anpassung LEIBER Group |
| 2.0 | 11.12.2025 | Udo Faulhaber | Kommunikation Richtlinie, Verantwortlichkeiten bei neuen Projekten |

Die Geschäftsführung der LEIBER Group GmbH & Co. KG in 78576 Emmingen-Liptingen, im Folgenden kurz „Organisation" genannt, verabschiedet diese Leitlinie zur Informationssicherheit und zum Datenschutz, kurz „Leitlinie Informationssicherheit". Diese ist Bestandteil des Informationssicherheits-konzepts der Organisation. Mit der Leitlinie Informationssicherheit bekennt sich die Geschäftsführung sichtbar zu ihrer Verantwortung für Informationssicherheit. Die Leitlinie Informationssicherheit ist eng verbunden mit der Etablierung eines Prozesses zur Gewährleistung der Informationssicherheit (Informationssicherheits-Managementsystem, kurz ISMS), welches von der Organisation umgesetzt wurde.

## 1. Einleitung

Die Organisation nutzt und verarbeitet eine Vielzahl von Informationen, um ihre Aufgaben und Pflichten gegenüber ihren Kunden, Vertragspartnern, Dienstleistern, Behörden und sonstigen Dritten zu erfüllen. Dabei verarbeitet sie auch sensible Informationen, die einen hohen Schutzbedarf aufweisen und die vor Verlust, Manipulation oder unberechtigter Kenntnisnahme durch Dritte besonders zu schützen sind. Dazu gehören personenbezogene Daten, vertrauliche Daten von Kunden sowie interne schutz-bedürftige Daten aus Entwicklung, Konstruktion, Produktion, Finanzen, Vertrieb und weiteren Bereichen. Dies bezieht sich neben digitalen Daten auch auf alle gedruckten und mündlichen Informationen.

Ein Schwerpunkt der zu schützenden Informationen ergibt sich dabei aus der Funktion der Organisation als Zulieferer für die Automotive Branche. Hierzu zählen zum Beispiel Technische Zeichnungen in einem frühen Entwicklungsstadium für die Erstellung von Mustern und Angeboten. Außerdem besteht hoher Schutzbedarf für Kunden aus anderen Bereichen mit entsprechenden Anforderungen an die Informationssicherheit.

Ebenso muss sichergestellt werden, dass die Produktion und die Kommunikationsinfrastruktur zwischen Organisation und Kunden jederzeit verlässlich verfügbar ist. Die Sicherheit von Informationen und der Informationstechnologie (IT) inklusive der Steuerungen von Maschinen und Anlagen (OT) spielt daher eine Schlüsselrolle für die Aufgabenerfüllung der Organisation.

Diese Leitlinie ist Teil des Informationssicherheitskonzepts der Organisation und soll die Sicherheitsstrategie und die Sicherheitsorganisation in übersichtlicher und einheitlicher Form darstellen. Das Informationssicherheitskonzept beinhaltet weitere Detaillierungen, insbesondere die IT-Rahmenrichtlinie und die nachrangigen IT-Richtlinien sowie technische und organisatorische Maßnahmen zur Erreichung der notwendigen Informationssicherheit.

## 2. Geltungsbereich

Diese Leitlinie gilt für die LEIBER Group GmbH & Co. KG (Emmingen-Liptingen) sowie die LEIBER Poland GmbH mit Niederlassung in Polen/ Ruda Śląska einschließlich aller Mitarbeitenden, Führungskräfte und externen Partner im jeweiligen Verantwortungsbereich.

Diese Leitlinie ist für alle Mitarbeitenden, Lieferanten und externen Partner, die auf IT-Systeme oder auf schützenswerte Informationen der Organisation Zugriff erhalten, verbindlich. Dazu kann diese Leitlinie, auch auszugsweise, an dritte Parteien weitergegeben werden. Sofern nichts anderes definiert ist, sind die primären Ansprechpartner innerhalb der Organisation, die für Kommunikation mit einem spezifischen Dritten verantwortlich sind, auch dafür zuständig diese Leitlinie zu kommunizieren, auch bei Änderungen.

## 3. Sicherheitsziele

Bei der Organisation genießen der Schutz personenbezogener Daten und die Informationssicherheit höchste Priorität. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten Informationen.

Informationssicherheit ist ein entscheidender Faktor, um langfristig die Wettbewerbsfähigkeit sicherzustellen. Zu den vordringlichen Zielen der Informationssicherheit gehört es daher, gesetzliche Anforderungen und die mit Kunden getroffenen Vereinbarungen zu erfüllen, die Lieferfähigkeit sicherzustellen, Innovationen zu sichern und damit wettbewerbsfähig zu bleiben.

Bei der Planung und Umsetzung ihrer Geschäftsprozesse gewährleistet die Organisation deshalb in allen Prozessen und Strukturen die Sicherstellung der Informationssicherheit. Hierbei müssen die zentralen Planungen und Vorgaben des Informationssicherheitsbeauftragten, des ISMS-Teams und der zentralen IT-Abteilung (IT) berücksichtigt werden. Informationssicherheit ist gegeben, wenn die Vertraulichkeit, Verfügbarkeit und Integrität der Daten in den informationsverarbeitenden und -lagernden Systemen gesichert ist. Sie dient dem Schutz vor Gefahren, der Vermeidung von Schäden und der Minimierung aller absehbaren Risiken.

- **Vertraulichkeit** bedeutet, dass ausschließlich berechtigte Personen und Anwendungen Zugriff auf die Informationen haben.
- **Verfügbarkeit** heißt, dass der Zugang zu Informationen und Anwendungen jederzeit möglich ist, wenn der Bedarf hierzu besteht.
- **Integrität** der Daten bedeutet, dass die Nachvollziehbarkeit der geschäftsrelevanten Prozesse sowie die Richtigkeit und Vollständigkeit der Daten gewährleistet ist.

Darüber hinaus sind alle Mitarbeitenden an sämtlichen Standorten der Organisation verpflichtet, die Sicherheitsziele vor Ort einzuhalten. Die konkreten Sicherheitsmaßnahmen sollen dabei in einem wirtschaftlich angemessenen Verhältnis zum Schutzbedarf der verarbeiteten Informationen und zur erforderlichen Arbeitseffizienz der Mitarbeitenden stehen. Hierzu werden im Rahmen des ISMS regelmäßig sowie anlassbezogen die Risiken für die Informationssicherheit erhoben und bewertet, sowie mit angemessenen Maßnahmen behandelt.

Alle Mitarbeitenden, alle verbundenen Gesellschaften, die Geschäftsführung und alle Dienstleister der Organisation sind sich ihrer Verantwortung für die Informationssicherheit, insbesondere für Informationen in ihrem Verantwortungsbereich, bewusst und haben die Leitlinie Informationssicherheit zu beachten und zu unterstützen.

Die Organisation dokumentiert eine detaillierte Übersicht über definierte Zielvorgaben im Bereich Informationssicherheit und Datenschutz in einer separaten „Liste der Anforderungen an das ISMS“. Diese beinhaltet rechtliche, vertragliche sowie eigene Sicherheitsziele und wird bei Bedarf angepasst und erweitert.

## 4. Sicherheitsorganisation

Verantwortlich für Informationssicherheit in der Organisation ist die Geschäftsführung. Die Geschäftsführung ist insbesondere verantwortlich für

- die Schaffung organisatorischer Rahmenbedingungen zur nachhaltigen Gewährleistung von Informationssicherheit,
- die Definition und Festlegung der erforderlichen Verantwortlichkeiten und Befugnisse,
- die Einrichtung eines Informationssicherheits-Managements und IT-Sicherheitskonzepts, kurz (ISMS),
- die Sicherstellung, dass die Anforderungen des ISMS in die Geschäftsprozesse integriert werden,
- die Umsetzung der vereinbarten Sicherheitsmaßnahmen einschließlich der Bereitstellung der erforderlichen Ressourcen und Kompetenzen,
- eine hinreichende und geeignete Dokumentation der IT-Infrastruktur sowie aller Sicherheitsvorkehrungen und Sicherheitsmaßnahmen,
- die Förderungen der fortlaufenden Verbesserung des ISMS.

Zur Erreichung der Informationssicherheitsziele ist ein Informationssicherheitsbeauftragter (ISB) benannt, der der Geschäftsführung unmittelbar unterstellt ist. Der ISB berät die Geschäftsführung in allen Belangen bei der Planung und Umsetzung der Informationssicherheit in der Organisation. Er berichtet in seiner Funktion regelmäßig über den Sicherheitsstatus der Organisation und anlassbezogen über Sicherheitsvorfälle unmittelbar an die Geschäftsführung. Die Ernennung des ISB wird in einer separaten Ernennungsurkunde schriftlich fixiert und im Geltungsbereich dieser Leitlinie durch die Geschäftsführung kommuniziert.

Die Geschäftsführung steuert die Organisation der Informationssicherheit im Geltungsbereich dieser Leitlinie und entwickelt sie kontinuierlich weiter. Sie benennt die Verantwortlichen und deren Verantwortlichkeiten.

Der ISB ist, soweit möglich, frühzeitig in Projekte einzubinden, die die Einführung neuer Soft- und IT-Hardware erfordern und dabei im Ergebnis vertrauliche oder schützenswerte Informationen erzeugt oder verarbeitet, um bereits in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Der verantwortliche Projektleiter ist verpflichtet, den ISB rechtzeitig über derartige Projekte zu informieren.

Sofern personenbezogene Daten betroffen sind, gilt gleiches für den Datenschutzbeauftragten (DSB) der Organisation. Dieser ist, soweit möglich, frühzeitig in solche Projekte einzubinden, um einen gesetzeskonformen Umgang mit personenbezogenen Daten sicherzustellen und spezifische Risiken der automatisierten Datenverarbeitung für die Rechte und Freiheiten der betroffenen Personen weitestgehend zu minimieren. Die Organisation achtet dabei auf datenschutzfreundliche Technik (Privacy by Design) und datenschutzfreundliche Voreinstellung der Datenverarbeitungsprogramme und -verfahren (Privacy by default).

Der Datenschutzbeauftragte und der Informationssicherheitsbeauftragte sind bei Bedarf in Audits einzubinden, die die Informationssicherheit betreffen. Der Datenschutzbeauftragter ist in beratender Funktion tätig und Ansprechpartner für die Geschäftsführung, die Mitarbeiter und die Arbeitnehmervertretung in allen Belangen des Datenschutzes. Weiter steht er externen Dienstleistern als Ansprechpartner in Datenschutzfragen zur Verfügung.

Als zentraler Ansprechpartner der Mitarbeiter und dritter Parteien zum Thema Informationssicherheit und Datenschutz ist die IT-Abteilung der Organisation definiert.

## 5. Sicherheitsmaßnahmen

Technische und organisatorische Maßnahmen werden in der Organisation auf der Basis einer Risikoeinschätzung in einem Maßnahmenplan festgelegt. Dazu gehören auch Regelungen für Mitarbeiter und externe Dienstleister, die in IT-Richtlinien und evtl. in Betriebsvereinbarungen dokumentiert sind. Diese IT-Richtlinien bzw. Betriebsvereinbarungen werden den Mitarbeitern der Organisation und externen Dienstleistern bekannt gegeben und sind für diese verbindlich.

Dies beinhaltet die folgenden technischen und organisatorischen Ziele und Maßnahmen:

- Organisation der Informationssicherheit im Geltungsbereich dieser Leitlinie,
- Sicherstellung der Personalsicherheit vor, während, bei Beendigung oder Änderung des Beschäftigtenverhältnisses,
- Werte und Informationen der Organisation sind identifiziert und angemessene Verantwortlichkeiten zu ihrem Schutz entsprechend ihrer Bedeutung sind festgelegt,
- Zugang zu Informationen und informationsverarbeitenden Einrichtungen werden kontrolliert und nach Berechtigungskonzepten eingeschränkt,
- Sicherstellung der Betriebssicherheit, insbesondere Schutz vor Schadsoftware, Datenverlust, Datendiebstahl, Integrität der IT-Systeme und Daten und deren Wiederherstellung im Desaster Recovery Fall, einschließlich der Notfallplanung und Handhabung von Informationssicherheitsvorfällen.

Damit definierte Sicherheitsmaßnahmen korrekt und zielführend von allen Mitarbeitern der Organisation umgesetzt werden können, wird das ISMS-Team weitere Richtlinien zum Umgang mit Informationen, IT-Systemen und -Anwendungen sowie anderen relevanten Themen dokumentieren und den Anwendern dieser Richtlinien in geeigneter Form kommunizieren.

## 6. Verbesserung der Sicherheit

Diese Informationssicherheitsleitlinie, die Anforderungen an das ISMS, die abgeleiteten Maßnahmen und Richtlinien werden regelmäßig auf ihre Aktualität und Wirksamkeit geprüft und angepasst. Zur Messung der Wirksamkeit wird das ISMS-Team die entsprechenden Prozesse durch interne Audits überprüfen. Die Geschäftsführung unterstützt die kontinuierliche Verbesserung des Sicherheitsniveaus. Alle Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen zu melden.

## 7. Schlussbestimmungen

Diese Leitlinie Informationssicherheit tritt mit Ihrer Bekanntgabe in Kraft. Diese Leitlinie wird in der jeweils aktuellen Version in der „1700 Übersichtsliste Dokumente“ veröffentlicht.

Verstöße gegen diese Leitlinie und andere mitgeltenden Dokumente können zu arbeitsrechtlichen und zivilrechtlichen Konsequenzen führen.

**Emmingen, den 17.12.2025**