Informationssicherheitsleitline der TLV Euro Engineering GmbH

Inhaltsverzeichnis

1. Ziel und Zweck

Die Informationssicherheitsleitlinie schafft die Grundlage für den Aufbau eines Informationssicherheitsmanagementsystems (ISMS), welches die Herstellung und den Erhalt des erforderlichen Sicherheitsniveaus aller Informationswerte im Verantwortungsbereich der TLV Euro Engineering GmbH gewährleistet. Das ISMS beinhaltet eine transparente Beschreibung des Aufbaus und der Organisation, sowie der Abläufe und Prozesse und weiteren Vorgaben und Regeln. Durch deren Berücksichtigung wird es möglich, die Planung, Umsetzung und Überprüfung von Sicherheitsmaßnahmen im Geltungsbereich zu gewährleisten. Das ISMS unterstützt die Geschäftsleitung des Unternehmens dabei, ihrer gesetzlichen Verantwortung für die Informationssicherheit gerecht zu werden.

Die Geschäftsführung und -leitung unterstützt und engagiert sich für Informationssicherheit durch die organisationsweite Veröffentlichung und Aufrechterhaltung dieser Leitlinie und weiterer ISMS-Richtlinien.

2. Geltungsbereich

Die Informationssicherheitsleitlinie gilt im Anwendungsbereich des ISMS der TLV Euro Engineering GmbH, Daimler-Benz-Str. 16-18, 74915 Waibstadt sowie für alle angestellten Mitarbeitenden, inklusive Auszubildendenden und Auftragnehmer, sowie sonstigen externe Dritte, die Einrichtungen oder Informationen der TLV Euro Engineering GmbH nutzen.

Werden externe Dritte mit der Erbringung von Leistungen beauftragt, ist durch vertragliche Vereinbarungen sicherzustellen, dass die Informationssicherheitsleitlinie in den Leistungsbeziehungen berücksichtigt wird.

3. Änderungsdienst

Dieses Dokument wird periodisch auf Aktualität und Vollständigkeit geprüft. Die Änderungen sind von der Geschäftsführung freizugeben und in der Änderungshistorie aufzuführen. Der Revisionsstand wird jeweils um eins erhöht.

4. Begriffe

In diesem Abschnitt sind die in der Leitlinie genannten Abkürzungen und Begriffe aufgelistet.

ISB = Informationssicherheitsbeauftragte/r

ISMS = Informationssicherheitsmanagementsystem

Integrität

… beschreibt die Eigenschaft von Informationen (Werten), dass sie vollständig und lediglich von berechtigten Personen oder Systemen auf genehmigte Weise abgeändert werden können.

Vertraulichkeit

… beschreibt Eigenschaft von Informationen (Werten), dass sie lediglich berechtigten Personen oder Systemen verfügbar gemacht werden.

Verfügbarkeit

… beschreibt die Eigenschaft von Informationen (Werten), auf Verlangen zugänglich und nutzbar zu sein.

5. Referenzdokumente

- Richtlinien der TLV Euro Engineering GmbH
- ISO / IEC 27001
- BSI IT-Grundschutz

6. Stellenwert der Informationssicherheit

Die Nutzung aktueller Informationstechnologien, um die Durchführung der unternehmerischen Aufgaben im Sinne der Kunden und Geschäftspartner effizient und effektiv abzuwickeln, sind fester Bestandteil des Arbeitsalltags. Die Informationssicherheit ist daher eine unverzichtbare Grundlage für die Erfüllung der Aufgaben innerhalb des Unternehmens.

Von besonderer Bedeutung sind die Informationswerte, wie Kundendaten, Mitarbeiterdaten und technische Daten, deren Schutz für das Ansehen und die Aufgabenerfüllung der TLV Euro Engineering GmbH maßgeblich sind.

Aufgaben, Prozesse und Aufbauorganisation unterliegen einem stetigen Wandel und einer Anpassung der technischen Möglichkeiten. In Abwägung der zu schützende Werten, der gesetzlichen Anforderungen und der damit verbundenen Risiken wird ein angemessenes Informationssicherheitsniveau geschaffen.

Es ist notwendig, das Zusammenspiel der Informationen, Aufgaben und Produkte sowie der Infrastruktur der Informationstechnik und Kommunikationskanäle ganzheitlich zu betrachten. Informationssicherheit umfasst die Summe aller organisatorischen, personellen und technischen Maßnahmen, um ein wirksames Sicherheitsniveau zu erreichen. Sowohl bei der Erbringung der Pflichtaufgaben als auch der Aufgaben, welche die TLV Euro Engineering GmbH auf freiwilliger Basis übernimmt, werden Informationen erhoben und verarbeitet, deren Vertraulichkeit, Integrität und Verfügbarkeit ein hohes Gut darstellen. Hierbei handelt es sich z.B. um Daten, die entsprechend gesetzlichen Anforderungen geschützt werden müssen, oder auch um wettbewerbsrelevante Informationen von Kunden und Partnern, die Unberechtigten nicht bekannt werden dürfen.

Beim Umgang mit Informationswerten aller Art muss die TLV Euro Engineering GmbH darauf achten, dass dem Schutzbedarf entsprechend Rechnung getragen wird.

Informationssicherheit und eine hohe Qualität in unseren Prozessen machen uns vertrauenswürdig, zuverlässig und sicher in der Zusammenarbeit mit Kunden und Geschäftspartnern.

7. Sicherheitsziele

Ziel dieser Informationssicherheitsleitlinie ist es, Aspekte der Informationssicherheit in jeden Prozess zu integrieren, um die Vertraulichkeit, die Integrität und die Verfügbarkeit der Informationswerte sicherzustellen.

Die Ausübung der Unternehmenstätigkeiten muss vor Bedrohungen von außen (z.B. aus dem Internet) und aus internen Quellen geschützt werden. Beispiele sind:

- Schutz vor Datendiebstahl oder ungewollter Offenlegung von Geheimnissen durch Schadsoftware
- Schutzvor Einschränkung der Arbeitsfähigkeit oder Nicht-Verfügbarkeit von Ressourcen durch Spam-E-Mail- oder Hacking-Attacken
- Schutz vor Identitäts-/ Datendiebstahl und ähnlichem.

So können die Werte der Vertraulichkeit, Verfügbarkeit und Integrität der Unternehmensdaten gewährleistet werden.

Schützenswertes Wissen umfasst Informationen und Daten, welche die Unternehmenstätigkeiten wesentlich bestimmen. Dies sind nicht nur geschriebene oder gedruckte Dokumente, sondern auch Informationen in anderer Form (z.B. elektronisch gespeicherte Daten, gesprochenes Wort usw.). Einbezogen sind deswegen alle Prozesse und Systeme der Informations- und Kommunikationstechnik, mit denen Informationen elektronisch gespeichert, verarbeitet oder übertragen werden.

Schützenswerte Informationswerte sind neben diesen Informationen und den für ihre Speicherung, Verarbeitung und Übertragung eingesetzten IT-Systemen insbesondere auch das Image der Firma und die mit dem Firmennamen in Beziehung gebrachten Produkte, Dienstleistungen und Personen.

Unsere Geschäftsprozesse müssen auf die Auswirkungen von Schäden, die durch Störungen oder sogar durch Notfallsituationen eintreten können, vorbereitet sein.

8. Verantwortung und Organisation

Die Geschäftsführung ist für die Informationssicherheit der TLV Euro Engineering GmbH verantwortlich und stellt sicher, dass entsprechend dieser Informationssicherheitsleitlinie das ISMS umgesetzt, betrieben und weiterentwickelt wird.

Die Geschäftsführung stellt die erforderlichen Ressourcen für den Aufbau und die Pflege des ISMS und die erforderliche Qualifikation der verantwortlichen Mitarbeiter bereit.

Die Geschäftsführung bewertet in regelmäßigen Abständen durch eine Managementbewertung das ISMS und legt Maßnahmen zur Optimierung fest.

Die Geschäftsführung legt für die TLV Euro Engineering GmbH die folgenden Grundsätze der Informationssicherheit fest:

- Verantwortung und Bewusstsein: Jeder Einzelne vermeidet in seinem Tätigkeitsbereich durch verantwortliches Handeln Schäden und meldet erkannte Schwachstellen umgehend.
- Steuerung und Risikoorientierung: Die Steuerung der Maßnahmen zur Erhöhung der Informationssicherheit erfolgt durch das Informationsrisikomanagement (IRM).

- Effizienz und Integration: Bei umzusetzenden Maßnahmen wird eine Aufwand-Nutzen-Betrachtung durchgeführt. Informationssicherheit muss über Fachbereiche hinweg etabliert werden. Stehen mehrere alternative Maßnahmen zur Erreichung eines Sicherheitsziels zur Verfügung, so wird die hinsichtlich der Investitionen und Betriebskosten wirtschaftlichste Maßnahme ausgewählt.
- Erfolgskontrolle und Qualität: Regelmäßige Erfolgskontrollen garantieren die Qualität und die kontinuierliche Verbesserung der Informationssicherheit.

9. Informationssicherheitsbeauftragte/r (ISB)

Die Geschäftsführung benennt schriftlich die/den Informationssicherheitsbeauftragten (ISB).

Die/der ISB ist in dieser Rolle der Geschäftsführung unterstellt und berichtet an die Geschäftsführung und -leitung. Die/der ISB ist für die Planung, Umsetzung, Aufrechterhaltung und Optimierung des ISMS verantwortlich.

Ein Austausch mit der Leitung der Informationstechnik findet regelmäßig statt.

Die/der ISB überprüft in regelmäßigen Abständen die Zielvorgaben, die Prozessparameter, Sicherheitsvorfälle und die Umsetzung der Maßnahmen.

Die/der ISB informiert die Geschäftsführung und -leitung bei Informationssicherheits- und Datenschutzvorfällen.

Die/der ISB überprüft das ISMS hinsichtlich der Umsetzung der Vorgaben in dieser Informationssicherheitsleitlinie mindestens einmal jährlich und im Falle von erheblichen Änderungen. Der Zweck dieser Überprüfung ist der Nachweis der Angemessenheit, Eignung und Wirksamkeit des ISMS.

Die/der ISB überprüft die internen Regelungen zur Informationssicherheit mindestens einmal jährlich auf Aktualität und Angemessenheit. Die Ergebnisse der Prüfung und eingeleitete Maßnahmen sind zu dokumentieren.

10. Sicherheitsorganisation (Ablauforganisation)

Die Sicherheitsorganisation umfasst alle Verantwortlichen und Beteiligten, die bei dem Aufbau und der Durchführung des ISMS mitwirken.

Um diese Anforderungen zu erfüllen, sind in einem IT-Sicherheitskonzept die Vorgaben und Maßnahmen für einen sicheren Einsatz von IT- und Informationssystemen zu dokumentieren.

Das IT-Sicherheitskonzept dient gleichzeitig der Optimierung der Informationssicherheit und trägt dazu bei, bestehende und künftige Prozesse im Hinblick auf eine sichere Verarbeitung der Daten weiter zu optimieren.

Für bereits betriebene und für geplante Informationsverarbeitung und Infrastrukturen sind IT-Sicherheitskonzepte zu erstellen.

IT-Sicherheitskonzepte beinhalten mindestens:

- eine Beschreibung der zur Datenverarbeitung eingesetzten technischen und organisatorischen Mittel (IT-Strukturanalyse oder IT-Konzept)
- eine Risikoanalyse auf Grundlage einer Schutzbedarfsfeststellung
- ein Risikobehandlungsplan (Liste technischer und organisatorischer Maßnahmen)

Bei der Auswahl geeigneter Maßnahmen im Rahmen einer Risikoanalyse werden neben der Wirksamkeit auch die Aspekte Benutzbarkeit (Usability) und Wirtschaftlichkeit berücksichtigt.

Der ISB ist bei allen organisatorisch-technischen Neuerungen oder Änderungen, die Auswirkungen auf die Informationssicherheit haben können, durch die Verantwortlichen der Fachbereiche und Abteilungen frühzeitig einzubinden.

11. Verpflichtung zur kontinuierlichen Verbesserung

Ein wesentliches Ziel des ISMS ist nicht nur das Erlangen und Halten eines definierten Sicherheitsniveaus, sondern dessen ständige Überprüfung und durch einen Prozess zur kontinuierlichen Verbesserung.

Für die Aufrechterhaltung der Sicherheit im laufenden Geschäftsbetrieb wird ein internes Kontrollsystem etabliert.

12. Maßnahmen bei Verstößen

Beabsichtigte oder grob fahrlässige Handlungen, die Sicherheitsvorgaben verletzen, können finanzielle Verluste bedeuten, Mitarbeiter, Geschäftspartner und Kunden schädigen oder den Ruf des Unternehmens TLV Euro Engineering GmbH gefährden. Bewusste Verstöße gegen verpflichtende Sicherheitsregeln können arbeitsrechtliche und unter Umständen auch strafrechtliche Konsequenzen haben und zu Regressforderungen führen.

13. Inkrafttreten

Hiermit wird die Informationssicherheitsleitlinie durch die Freigabe der Geschäftsführung in Kraft gesetzt.

Waibstadt, 06.02.2025

Reiner Weiß
Geschäftsführer

ppa. G. Di Marco
Gregorio Di Marco
Prokurist

Erstellt:	01.02.2025	Dr. M. L. Winnertz	**Rev:**	01
Geprüft:	06.02.2025	G. Di Marco	**Vertraulichkeit**	Öffentlich
Freigegeben:	06.02.2025	R. Weiß		
Dateiname:	TLV Euro Engineering GmbH | IT Sicherheitsleitlinie			