INFORMATIONSSICHERHEITS-LEITLINIE

VOIT AUTOMOTIVE

Stand: 02.05.2023

Ordnungs-Nr.: LL 01.01
Rev.: 02

Inhaltsverzeichnis

Gliederung der nachfolgenden Informationssicherheitsleitlinie: Seite

Informationssicherheitsleitlinie

1. Ziel und Zweck

Die Informationssicherheitsleitlinie schafft die Grundlage für den Aufbau eines Informationssicherheitsmanagementsystems (ISMS), das die Herstellung und den Erhalt des erforderlichen Sicherheitsniveaus aller Informationswerte im Verantwortungsbereich der VOIT Automotive GmbH sicherstellt. Das ISMS beinhaltet Aufbauorganisation, Ablauforganisation (Prozesse) und Regelwerk, die geeignet sind, Planung, Umsetzung und Überprüfung von Sicherheitsmaßnahmen im Geltungsbereich zu gewährleisten. Das ISMS unterstützt die Leitung 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 VOIT Automotive GmbH, Saarbrücker Straße 2, nebst den Werken 2 & 3, D-66386 St. Ingbert und für alle angestellten Mitarbeiter, inklusive der leitenden Angestellten i.S.d. § 5 Abs. 3 BetrVG, Auszubildende und Auftragnehmer, sowie sonstige externe Dritte, die Einrichtungen oder Informationen der VOIT Automotive GmbH nutzen.

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

3. Änderungsdienst

Dieses Dokument wird jährlich auf Aktualität und Vollständigkeit überprüft. Die Verantwortung zur Pflege und Anpassung liegt beim Informationssicherheitsbeauftragten. Das geänderte Dokument wird komplett ausgetauscht. 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 = Informationssicherheitsbeauftragter
ISMS = Informationssicherheitsmanagementsystem

Verfügbarkeit
Die Eigenschaft von Informationen (Werten), auf Verlangen zugänglich und nutzbar zu sein.

Integrität
Die Eigenschaft von Informationen (Werten), dass sie lediglich von berechtigten Personen oder Systemen auf genehmigte Weise abgeändert werden können.

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

5. Referenzdokumente

- VDA-TISAX (Trusted Information Security Assessment Exchange)
- ISO/IEC 27001
- ISMS Anwendungsbereich der VOIT Automotive GmbH
- Anwendbarkeitserklärung der VOIT Automotive GmbH
- Richtlinien der VOIT Automotive GmbH

6. Bedeutung der Informationssicherheit

Moderne Unternehmen sind geprägt von dem Einsatz aktueller Informationstechnologien, um die Durchführung der unternehmerischen Aufgaben im Sinne ihrer Kunden und Geschäftspartner effizient und effektiv abzuwickeln. 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 VOIT Automotive GmbH maßgeblich sind.

Aufgaben, Prozesse und die Aufbauorganisation unterliegen einem stetigen Wandel und einer Anpassung der technischen Möglichkeiten. In Abwägung der zu schützenden Werte, 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 VOIT Automotive 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 VOIT Automotive GmbH darauf achten, dass dem Schutzbedarf entsprechend Rechnung getragen wird.

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. Dieser Schutz soll z.B. vor Datendiebstahl oder ungewollter Offenlegung von Geheimnissen durch Schadsoftware, vor Einschränkung der Arbeitsfähigkeit oder Nicht-Verfügbarkeit von Ressourcen durch Spam-E-Mail oder Hacking-Attacken, vor Identitäts-/ Daten-Diebstahl und Ähnlichem wirken.

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

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

8. Verantwortung und Organisation

Die Geschäftsführung ist für die Informationssicherheit der VOIT Automotive 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 VOIT Automotive 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 Kosten-Nutzen-Betrachtung durchgeführt. Informationssicherheit ist eine Querschnittsfunktion über alle Fachbereiche hinweg. 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. Informationssicherheitsbeauftragter (ISB)

Die Geschäftsführung benennt schriftlich als zentrale Sicherheitsinstanz den Informationssicherheitsbeauftragten (ISB) und dessen Stellvertreter.

Der ISB ist in dieser Rolle der Geschäftsführung unterstellt und berichtet an die Geschäftsführung und -leitung.

Der ISB ist für die Planung, Umsetzung, Aufrechterhaltung und Optimierung des ISMS verantwortlich.

Ein Austausch mit der Leitung der Informationstechnik findet regelmäßig statt.

Der ISB überprüft in regelmäßigen Abständen die Zielvorgaben, die Prozesskennzahlen, Sicherheitsvorfälle und die Umsetzung der Maßnahmen.

Der ISB informiert die Geschäftsführung und -leitung bei Informationssicherheits- und Datenschutzvorfällen.

Der ISB überprüft (auditiert) 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.

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 Erreichen und Aufrechterhalten eines definierten Sicherheitsniveaus, sondern dessen ständige Anhebung durch einen Prozess zur kontinuierlichen Verbesserung.

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

12. Maßnahmen bei Verstößen

Verstöße gegen diese Informationssicherheitsleitlinie sowie Richtlinien und sonstige Vorschriften können zu erheblichen negativen Konsequenzen für die VOIT Automotive GmbH führen. Deshalb ist bei vorsätzlichen und grob fahrlässigen Handlungen, die einen Verstoß darstellen, mit arbeitsrechtlichen Konsequenzen zu rechnen.

Darüber hinaus können derartige Zuwiderhandlungen auch straf- oder zivilrechtliche Schritte nach sich ziehen.

13. Inkraftsetzung

Hiermit wird die Informationssicherheitsleitlinie durch die Freigabe der Geschäftsführung in Kraft gesetzt und wird allen interessierten Parteien (u.a. Mitarbeiter und Kunden) nach Unterschrift umgehend zur Kenntnis gebracht.

St. Ingbert, den 02.05.2023

Hendrik Otterbach
CFO - Chief Financial Officer

Christopher Pajak
CCO - Chief Corporate Officer

14. Revisions-Historie

Freigabedatum:	Revision:	Erstellt durch:	Beschreibung der Änderung:
02.05.2023	02	Andrea Geimer	Aktualisierung der Unterschriftszeile
18.02.2022	01	Andrea Geimer	Erstellung der Informationssicherheitsleitlinie

Erstellt/Geändert am: 02.05.2023	**Geprüft am:** 02.05.2023	**Freigegeben am:** 02.05.2023	**Rev.:** 02
von: ISB Andrea Geimer	**von:** GL Alexander Wörner	**von:** GF Hendrik Otterbach	