Leitlinie Informationssicherheit

Informationen zur Prävention von und zum Umgang mit Informationssicherheitsverstößen

Ziel und Zweck

Dieses Dokument beschreibt die Management-Vorgaben für die Informationssicherheit des Informationssicherheitsmanagementsystems (ISMS) im geltenden Anwendungsbereich und die Informationssicherheitsziele der CarGarantie.
Ziel der vorliegenden Leitlinie ist die Richtungsvorgabe und Unterstützung durch den Vorstand bei der wirksamen Umsetzung der Informationssicherheit in Übereinstimmung mit Geschäftsanforderungen und geltenden Gesetzen und Regelungen.
Diese Leitlinie kann auch allen externen interessierten Parteien wie Kunden und Lieferanten zur Verfügung gestellt werden.

Motivation

Der Vorstand der CarGarantie unterstützt und engagiert sich für Informationssicherheit durch die organisationsweite Veröffentlichung und Aufrechterhaltung dieser und weiterer Richtlinien.
Die Informationstechnologie (IT) spielt eine zentrale Rolle in der Durchführung der Geschäftsprozesse der CarGarantie, welches durch die zunehmende Digitalisierung verstärkt wird. Dies gilt gleichermaßen für die unternehmensinternen Prozesse wie auch für die Prozesse, die für die Zusammenarbeit mit Herstellern, Händlern, Banken und Partnern notwendig sind.
Die CarGarantie entwickelt die Wirksamkeit unserer Geschäftsprozesse durch den Einsatz moderner Mittel der Informations- und Kommunikationstechnik kontinuierlich weiter. Informationssicherheit bedeutet für uns, dass unsere Prozesse unter Minderung der unvermeidbaren Restrisiken

- den Schutz vertraulicher Informationen sicherstellen,
- die Integrität der Daten gewährleisten,
- bei Bedarf verfügbar sind und
- zuverlässig funktionieren.

Geltungsbereich

Dieses Dokument gilt im Anwendungsbereich des ISMS der CarGarantie Freiburg und somit für alle angestellten Mitarbeitenden und Auftragnehmer sowie sonstige externe Dritte, die Einrichtungen oder Informationen der CarGarantie nutzen.

Sicherheitsziele

Die Informationssicherheit der CarGarantie verfolgt das Ziel, verarbeitete Informationen jeglicher Art und Herkunft entsprechend ihrer Klassifizierung zu schützen. Informationen sind auf Papier, in IT-Systemen oder auch in den Köpfen der Benutzer gespeichert, wobei die Grundwerte Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität gewährleistet werden.
Ein stabiles Sicherheitsniveau wird durch ein geplantes und abgestimmtes Vorgehen aller Beteiligten erreicht und aufrechterhalten. CarGarantie etabliert ein wirksames Informationssicherheitsmanagementsystem, durch welches die Themen der Informationssicherheit und des Risikomanagements aktiv unterstützt werden

Die CarGarantie etabliert ein Informationssicherheitsmanagement auf Basis ISO 27001 und BSI IT-Grundschutz, welches über die Phasen Planung, Umsetzung, Erfolgskontrolle sowie Optimierung (Plan-Do-Check-Act) regelmäßig überprüft und kontinuierlich verbessert wird. CarGarantie verfolgt hiermit zwei Ziele:

- Das Sicherheitsniveau muss den aktuellen Schutzbedarf der von den Informationen abhängigen bzw. auf IT gestützten Geschäftsprozesse abdecken. Sowohl in der CarGarantie als auch bei der Einbeziehung von Dienstleistern ist die bedarfsgerechte Verfügbarkeit von Informationen bzw. IT-Diensten sicherzustellen und die Vertraulichkeit, Integrität und Authentizität der verarbeiteten Informationen angemessen zu gewährleisten. Besonders der zunehmenden Bedrohung durch Cyberangriffe ist adäquat zu begegnen.
- Die Sicherheitsmaßnahmen werden so gestaltet, dass die CarGarantie ihre gesetzlichen, aufsichtsrechtlichen und vertraglichen Pflichten erfüllt. Interne Regelungen und Richtlinien werden beachtet.

Verantwortung und Organisation

Der Vorstand ist für die Informationssicherheit der CarGarantie verantwortlich und stellt sicher, dass entsprechend dieser Leitlinie das ISMS umgesetzt und betrieben wird und dass alle notwendigen Ressourcen verfügbar sind.
Informationssicherheit ist eine ganzheitliche und strategische Aufgabe, die von allen Mitarbeitern ein verantwortungsbewusstes und engagiertes Handeln erfordert. Dies bezieht sich insbesondere auch auf die Meldung von und den Umgang mit Informationssicherheitsvorfällen.
Durch geeignete Qualifizierungs- und Sensibilisierungsmaßnahmen zu Themen der Informationssicherheit, zum Datenschutz sowie zu den entsprechenden ISMS-Richtlinien und sonstigen Vorschriften wird das Sicherheitsbewusstsein der Mitarbeiter kontinuierlich aufrechterhalten und weiterentwickelt.
ISMS-Maßnahmen werden nach Beschluss bzw. Freigabe unter Maßgabe der Einhaltung einschlägiger rechtlicher, vertraglicher und interner Regelungen realisiert. Ihrer Berücksichtigung wird hohe Priorität beigemessen.
Bei Änderungen der Gesetzeslage werden die ISMS-Vorgaben zügig aktualisiert.
Diese Informationssicherheitsleitlinie wird durch weitere Richtlinien unterstützt und durch konkrete dokumentierte Informationen (Arbeitsanweisungen, Vorlagen) operationalisiert. Alle Dokumente für das ISMS unterliegen einer Lenkung.

Informationssicherheitsbeauftragter (ISB)

Der Vorstand benennt schriftlich den Informationssicherheitsbeauftragten, der direkt an den Vorstand berichtet.
Der ISB ist für die Planung, Umsetzung, Aufrechterhaltung und Optimierung des Informationssicherheitsmanagementsystems verantwortlich.
Ein Stellvertreter des Informationssicherheitsbeauftragten wird benannt.
Der Vorstand stellt der Informationssicherheitsorganisation ausreichende Ressourcen in Form von Personal, Zeit und Geld zur Verfügung.
Der Informationssicherheitsbeauftragte muss das ISMS hinsichtlich der Umsetzung der Vorgaben in dieser Leitlinie mindestens einmal jährlich und im Falle von erheblichen Änderungen überprüfen und den Status dokumentieren. Zweck dieser Überprüfung ist der Nachweis der Angemessenheit, Eignung und Wirksamkeit des ISMS.

Persönliche Verantwortung jedes Mitarbeiters

Die Geschäftsführung legt für die CarGarantie 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.
- Erfolgskontrolle und Qualität: Regelmäßige Erfolgskontrollen garantieren die Qualität und die kontinuierliche Verbesserung der Informationssicherheit.

Maßnahmen bei Verstößen

Verstöße gegen diese Leitlinie sowie Richtlinien und sonstige Vorschriften können zu erheblichen negativen Konsequenzen für CarGarantie 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.

Ansprechpartner

Der Informationssicherheitsbeauftragte ist der zentrale Ansprechpartner für alle Belange der Informationssicherheit, zu erreichen über informationssicherheit@cargarantie.com.