Version: 2.3
Status: Final
Datum: 07.09.2023
Eigentümer: Sven Hahn
Klassifizierung: Öffentlich

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 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 Leit- und 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.
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 und Authentizität der Daten gewährleisten,
- bei Bedarf verfügbar sind und
- zuverlässig funktionieren.

Geltungsbereich

Diese Leitlinie gilt sowohl für alle Mitarbeiter:innen der CarGarantie als auch für Auftragnehmer und 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 Mitarbeiter:innen und Lieferanten gespeichert, wobei die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit 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 Informationssicherheit und das Risikomanagement aktiv unterstützt werden.
Die CarGarantie etabliert ein Informationssicherheitsmanagement auf Basis der international anerkannten Norm DIN ISO/IEC 27001, 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 sowie die Vertraulichkeit und Integrität 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.

CarGarantie erreicht diese Sicherheitsziele, indem in weiteren Leit- und Richtlinien die ISMS-Prozesse sowie Vorgaben zur Maßnahmenumsetzung festgelegt werden. Die definierten technologischen und organisatorischen Maßnahmen werden operativ umgesetzt. Für Lieferanten werden dieselben Anforderungen an das einzuhaltende Sicherheitsniveau gestellt.

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.
Die Führungsebene der CarGarantie verpflichtet sich, in besonderem Maße auf die Einhaltung der Regelungen zur Informationssicherheit bei den Mitarbeiter:innen zu achten.
Informationssicherheit ist eine ganzheitliche Querschnittsfunktion für alle Tätigkeitsgebiete und eine strategische Aufgabe, die von allen Mitarbeiter:innen ein verantwortungsbewusstes und engagiertes Handeln erfordert. Jede(r) Einzelne vermeidet in seinem Tätigkeitsbereich durch verantwortliches Handeln Schäden und meldet erkannte Schwachstellen umgehend. Mitarbeiter:innen sind verpflichtet, Informationssicherheitsvorfälle umgehend zu melden.
Durch geeignete Qualifizierungs- und Sensibilisierungsmaßnahmen zu Themen der Informationssicherheit, zum Datenschutz, zur Compliance sowie zu den entsprechenden ISMS-Richtlinien und sonstigen Vorschriften wird das Sicherheitsbewusstsein der Mitarbeiter:innen aufrechterhalten und kontinuierlich weiterentwickelt.
ISMS-Maßnahmen werden unter 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 werden gelenkt.

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 finanziellen Mitteln zur Verfügung.
Der Informationssicherheitsbeauftragte muss das ISMS hinsichtlich der Umsetzung der Vorgaben in dieser Leitlinie mindestens einmal jährlich und im Falle von wesentlichen Änderungen überprüfen und den Status dokumentieren. Zweck dieser Überprüfung ist der Nachweis der Angemessenheit, Eignung und Wirksamkeit des ISMS.
Der Informationssicherheitsbeauftragte berichtet mindestens vierteljährlich und anlassbezogen dem Gesamtvorstand über den aktuellen Zustand des ISMS. Hierbei liegt ein besonderer Fokus auf Bedrohungen, Informationssicherheitsvorfällen, Informationsrisiken und umzusetzende Maßnahmen.

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** oder telefonisch unter +49 761 4548-0.