Leitlinie Informations-sicherheit

TECHNIK BRAUCHT SICHERHEIT

Inhaltsverzeichnis

FE/GF
Öffentlich

1 Einleitung

Im Rahmen der unternehmerischen Sorgfaltspflicht und im Hinblick auf die Erfüllung der Anforderungen der Informationssicherheit haben wir uns - die Geschäftsführung in Zusammenarbeit mit dem Führungskreis 1 – zum Aufbau, Betrieb und der fortlaufenden Verbesserung eines Informationssicherheits-Managementsystems (ISMS) verpflichtet. Das ISMS steht im Einklang mit der geschäftlichen Ausrichtung der GTÜ und ist in der Unternehmensstrategie verankert.
Dazu haben wir im Folgenden die Leitlinien und Ziele der Informationssicherheit festgelegt und stellen fortwährend die Integration der Informationssicherheit in die Geschäftsprozesse sowie die ausreichende Verfügbarkeit aller notwendigen Ressourcen sicher. Wir unterstützen alle Mitarbeitenden, Führungskräfte und interessierten Parteien, die zum Aufbau und wirksamen Betrieb beitragen und leiten diese an. Weiterhin überprüfen wir die Wirksamkeit und den Erfolg des ISMS.

2 Ziel und Zweck

Die GTÜ mbH ist eine jeweils durch die DAkkS nach DIN EN ISO/IEC 17020 (Inspektionsstellen) und ISO/IEC 17025 (Prüf- und Kalibrierlabore) zertifizierte Organisation, deren Geschäftszweck die Bereitstellung von Zertifizierungs-, Inspektions- und Prüfdienstleistungen in den Bereichen Automobil- und Verkehrssicherheit.
Das Portfolio umfasst weiterhin unterstützende Prozesse wie die Bereitstellung digitaler Dienstleistungen für Kunden und Partner. Das Geschäftsfeld schließt sowohl freiwirtschaftliche Bereiche als auch die Gewährleistung der öffentlichen Sicherheit in staatsentlastendem Auftrag ein.
Die Informationssicherheit spielt eine zentrale Rolle in der Erfüllung unserer Aufgaben, da die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und das damit verbundene Vertrauen in unsere Leistungsfähigkeit sowohl für hoheitliche als auch für kommerzielle Zwecke von höchster Bedeutung ist.
Diese Leitlinie ist gemäß den Anforderungen der ISO/IEC 27001:2022 (Kapitel 5.2) erstellt worden und legt die Leitlinien und Ziele für den Schutz von Informationen fest, die in unserer Organisation verarbeitet werden.

3 Geltungsbereich

Diese Leitlinie gilt für jeden Mitarbeitenden aller Geschäftsbereiche der GTÜ mbH und deren Tochtergesellschaften GTÜ Anlagensicherheit GmbH, GTÜ Certification GmbH und GTÜ Prüfmittelservice GmbH (kurz GTÜ) ohne zeitliche Begrenzung, insbesondere für:

+ Prüfdienstleistungen im Automobil- und Verkehrssicherheitssektor sowie der Anlagensicherheit
+ Bereitstellung und Verwaltung von digitalen und analogen Dienstleistungen

- Schutz der Informationen in den Bereichen der Prüf-, Zertifizierungs- und IT-Dienstleistungen sowie in allen verbundenen Geschäftstätigkeiten.
- Durchführung aller Dienstleistungen im Bereich „Technischer Dienst"

4 Grundsätze und Ziele

Die GTÜ verpflichtet sich, alle erforderlichen Maßnahmen zu ergreifen, um ein angemessenes Niveau der Informationssicherheit zu gewährleisten. Dies umfasst den Schutz aller sensiblen Informationen. Um unsere hoheitlichen Aufgaben und die freiwirtschaftlichen Dienstleistungen für unsere Kunden auf höchstem Niveau zu gewährleisten, verfolgen wir die folgenden Grundsätze und Informationssicherheitsziele:

- **Sicherstellung der Vertraulichkeit sensibler Daten**: nur autorisierte Personen haben Zugang zu sensiblen und vertraulichen Informationen. Insbesondere im Bereich der hoheitlichen Tätigkeiten müssen sensible Daten wie Prüfergebnisse, Zertifizierungen und interne Analysen vor unbefugtem Zugriff geschützt werden.
- **Schutz der Integrität alle Informationen**: Gewährleistung der Genauigkeit und Vollständigkeit der Informationen und Verhinderung unautorisierter Änderungen. Alle Prüf- und Zertifizierungsergebnisse müssen vor Manipulation geschützt sein, um die Glaubwürdigkeit der Prüfergebnisse sicherzustellen.
- **Maximierung der Verfügbarkeit**: Sicherstellung, dass Informationen und Dienstleistungen stets dann für befugte Personen zugänglich sind, wenn sie benötigt werden. Unsere digitalen Plattformen müssen in den Servicezeiten stabil und performant verfügbar sein, um beispielsweise unterbrechungsfreie Prüf- und Auftragsabwicklungen zu gewährleisten. Dazu gehört auch ein effektives Notfallmanagementsystem.
- **Rechtliche Konformität sicherstellen**: Sicherstellung der Einhaltung aller relevanten Gesetze, Vorschriften und vertraglichen Verpflichtungen, insbesondere in Bezug auf Datenschutz und staatliche Vorgaben.
- **Kontinuität, Risikomanagement und kontinuierliche Verbesserung**: Ein etabliertes Risikomanagement soll Bedrohungen und Schwachstellen identifizieren, bewerten und geeignete Maßnahmen zur Minimierung von Risiken einleiten. Dabei soll die Wirksamkeit regelmäßig überprüft und an neue Bedrohungslagen angepasst werden. Die Maßnahmen sollen sicherstellen, dass auch im Falle eines Sicherheitsvorfalls oder Ausfalls die geschäftliche Tätigkeit fortgesetzt werden kann.
- **Sensibilisierung und Schulung**: Schulung aller Beteiligten in Bezug auf die Bedeutung der Informationssicherheit und deren Verantwortung zur Einhaltung dieser Leitlinie. Alle Personen, die mit Informationen in Berührung kommen, müssen regelmäßig geschult werden, um die Risiken

und Maßnahmen der Informationssicherheit zu verstehen und anzuwenden.

+ **Sicherstellung der Nachvollziehbarkeit und Überprüfbarkeit von Prozessen**: Alle Informationssicherheitsprozesse müssen nachvollziehbar dokumentiert und überprüfbar sein, um sowohl interne als auch externe Audits zu ermöglichen.

6 Verantwortung und Zuständigkeit

Die Geschäftsführung der GTÜ mbH ist für die Informationssicherheit verantwortlich und hat das Informationssicherheits-Managementsystem (ISMS) gemäß TISAX® und ISO 27001:2022 beauftragt, implementiert und freigegeben. Weiterhin stellt die Unternehmensleitung ausreichende Mittel für die Aufrechterhaltung und die Verbesserung des ISMS zur Verfügung.
Die Leitlinie wird unter anderem durch zentral verfügbare Informationssicherheits-Richtlinien umgesetzt, in denen zielgruppen- und themenspezifische Vorgaben für die Umsetzung und Einhaltung der Informationssicherheit organisatorisch geregelt sind. Alle Mitarbeitenden und Dienstleister sind verpflichtet, die Informationssicherheitsrichtlinien und -verfahren einzuhalten.
Ein speziell ernannter Informationssicherheitsbeauftragter (ISB) überwacht die Einhaltung der Sicherheitsmaßnahmen, führt regelmäßige Schulungen durch und ist für die Berichterstattung an die Geschäftsführung verantwortlich.
Die Mitarbeitenden sind arbeitsvertraglich zur Einhaltung der Unternehmensrichtlinien verpflichtet. Verstöße gegen diese Richtlinien können arbeitsrechtliche, strafrechtliche und zivilrechtliche Konsequenzen nach sich ziehen.

7 Überwachung und Verbesserung

Die Unternehmensleitung überprüft und bewertet in regelmäßigen Management-Reviews die Wirksamkeit des ISMS unter Berücksichtigung interner und externer Audits, Risiko, Kennzahlen und Sicherheitsvorfällen hinsichtlich seiner Wirksamkeit. Es wird ein kontinuierlicher Verbesserungsprozess (KVP) umgesetzt, um neue Risiken und technologische Entwicklungen zu adressieren und sicherzustellen, dass unsere Informationssicherheitsziele erreicht werden.

8 Gültigkeit und Überprüfung der Leitlinie

Diese Informationssicherheitsleitlinie tritt mit ihrer Veröffentlichung in Kraft und wird mindestens jährlich überprüft und bei Bedarf aktualisiert, um sicherzustellen, dass sie den aktuellen Anforderungen entspricht und die Informationssicherheitsziele weiterhin erfüllt werden.

*) Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Technik braucht Sicherheit.

GTÜ Gesellschaft für
Technische Überwachung mbH
Vor dem Lauch 25
70567 Stuttgart

FON 0711 97676-0
MAIL info@gtue.de
WEB www.gtue.de