

Leitlinie zur Informationssicherheit

Ingenieurbüro für KFZ-Technik GmbH

Schmidt – Elsner – Espe

Alte Frankfurter Straße 211

D-38122 Braunschweig



Inhalt

1	Einleitung.....	4
1.1	Ingenieurbüro für KFZ-Technik GmbH.....	4
1.2	Geltungsbereich	4
1.3	Ansprechpartner.....	4
1.4	Verantwortlichkeiten	4
2	Stellenwert der IT-Technologie und Informationssicherheit.....	4
3	Unternehmensziele	5
3.1	Einhaltung von Gesetzen oder Vorschriften	5
3.2	Bewusstsein für Informationssicherheit	5
3.2.1	Vermeidung materieller Schäden	6
3.2.2	Wahrung von Persönlichkeitsrechten und Betriebsgeheimnissen	6
3.2.3	Vermeidung von Ansehensverlust bzw. Imageschaden.....	6
3.3	Kontinuierliche Verbesserung	6
3.4	Aktualisierung und Information.....	6
4	Konsequenzen bei Nichtbeachtung des ISMS.....	6
5	Rahmenwerk des ISMS.....	7
6	Regelmäßige Überprüfung dieser Leitlinie.....	7
7	Bereitstellung dieser Leitlinie	7

In diesem Dokument wird aus Gründen der besseren Lesbarkeit das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint, soweit es für die Aussage erforderlich ist und Personenbezeichnungen gelten gleichwohl für alle Geschlechter.

1 Einleitung

Die Geschäftsführung der Ingenieurbüro für Kfz-Technik GmbH, kurz Kfz-Büro, ist sich der Bedeutung der Informationssicherheit bewusst und erklärt diese zum integralen Bestandteil der Unternehmensstrategie.

Mit dieser Leitlinie werden grundsätzliche Werte und Ziele des Kfz-Büros im Bereich der Informationssicherheit definiert und sie bringt, entsprechend ISO 27001 Klausel 5, die Verpflichtung der Geschäftsführung zum Ausdruck.

Aufgrund der permanenten Weiterentwicklung in der Informationstechnologie unterliegen diese Leitlinie zur Informationssicherheit und alle darauf aufbauenden Richtlinien und Konzepte der fortlaufenden Anpassung und Weiterentwicklung.

Die Leitlinie zur Informationssicherheit ist für alle Beschäftigten des Kfz-Büros, in elektronischer und/oder gedruckter Form, einsehbar. Für interessierte Parteien des Unternehmens ist diese Leitlinie im Internet veröffentlicht.

1.1 Ingenieurbüro für Kfz-Technik GmbH

Das Ingenieurbüro für Kfz-Technik GmbH gehört zu den etabliertesten Kfz-Gutachtern und Sachverständigen in der Region Braunschweig. Ob Kfz-Bewertung, Unfallgutachten, Wertermittlung von Oldtimern oder Erstellung neutraler Gutachten für Leasingnehmer und Leasinggeber – seit mehreren Jahrzehnten vertrauen Privatpersonen und gewerbliche Kunden auf unsere Kompetenz. Mit ihren vier Standorten in Braunschweig, Wernigerode, Osterode und Goslar ist sie eines der größten und damit flexibelsten Kfz-Sachverständigenbüros im PLZ-Gebiet 38.

Alle Kunden, Geschäftspartner und Beschäftigte müssen sich darauf verlassen können, dass das Kfz-Büro ihre Sicherheitsverantwortung, für die von ihr verarbeiteten Informationen gewissenhaft wahrnimmt und Informationen vor missbräuchlicher Verwendung schützt.

Zur Erreichung der Informationssicherheitsziele wurde eine Sicherheitsorganisation, bestehend aus Informationssicherheits- und Datenschutzbeauftragten, eingerichtet.

1.2 Geltungsbereich

Die Leitlinie zur Informationssicherheit gilt für alle Standorte und alle Mitarbeiter des Kfz-Büros. Diese Leitlinie zur Informationssicherheit erstreckt sich auf alle Informationen, die von oder mit IT-Systemen und nicht IT-Systemen verarbeitet werden. Darüber hinaus können weitere Richtlinien und Regelungen gelten, die den Anwendungsbereich betreffen.

1.3 Ansprechpartner

Ansprechpartner zu allen Fragen dieser Leitlinie ist der Informationssicherheitsbeauftragte (ISB), welcher direkt an die Geschäftsführung berichtet und die Geschäftsführung selbst.

1.4 Verantwortlichkeiten

Diese Leitlinie hat die Geschäftsführung des Kfz-Büros genehmigt und freigegeben. Die Beachtung, Verteilung und Umsetzung dieser Leitlinie obliegt der Verantwortung des ISB.

2 Stellenwert der IT-Technologie und Informationssicherheit

Die Informationssicherheit sowie Informationstechnologie (IT) hat im Kfz-Büro einen sehr hohen Stellenwert und stellt ein wichtiges Qualitätsmerkmal der Datenverarbeitung dar, da viele wesentliche

strategische und operative Geschäftsprozesse durch Informationstechnologien maßgeblich unterstützt werden.

Ziel des KFZ-Büros ist es, die Daten und IT-Systeme über alle Geschäftsprozesse in ihrer Verfügbarkeit so zu sichern, so dass die Integrität und Vertraulichkeit von sensiblen Unternehmens- und personenbezogenen Daten in ausreichender Weise garantiert sind. Schadensfälle mit hohen finanziellen Auswirkungen und immaterielle Folgen in Form von Imageschäden für das Unternehmen müssen verhindert werden. Beeinträchtigungen hinsichtlich der Verfügbarkeit der unternehmenseigenen Applikationen können ebenso gravierende Auswirkungen nach sich ziehen wie Unregelmäßigkeiten in Bezug auf die Integrität und Vertraulichkeit der verarbeiteten bzw. benutzten Informationen. Die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen, Anwendungen und IT-Systeme werden nicht nur durch Externe bedroht, sondern können auch durch interne Schwachstellen gefährdet werden. Ferner werden der Informationssicherheit im Hinblick auf Ausschreibungen Vorteile im Markt eingeräumt.

3 Unternehmensziele

Die Geschäftsführung des KFZ-Büros hat entschieden, dass ein angemessenes Sicherheitsniveau für einen sehr hohen Schutzbedarf angestrebt werden soll. Grundlage für diese Entscheidung war eine Risikoanalyse über die Werte der zu schützenden Güter sowie des vertretbaren Aufwands an Personal und Finanzmitteln für Informationssicherheit.

Als strategische Ziele hat die Geschäftsführung beschlossen:

- die Einführung eines Informationssicherheitsmanagementsystems (ISMS),
- die Zertifizierung des Standortes Braunschweig,
- die Vermittlung der Notwendigkeit zur aktiven Unterstützung der Informationssicherheit in Form von Schulungen der Mitarbeiter,
- Vertraulichkeit der Informationen
- Integrität der Informationen
- Verfügbarkeit der Informationen

3.1 Einhaltung von Gesetzen oder Vorschriften

Die Maßnahmen zur Informationssicherheit sollen dazu beitragen, dass die für das Unternehmen relevanten Gesetze, Vorschriften und vertraglichen Verpflichtungen von Mitarbeitern und Organen eingehalten werden. Die Gesetze sind nachfolgend geregelt:

- Datenschutzgrundverordnung (DSGVO)
- Einhaltung des VDA-ISA in Schrift und Form (TISAX®)

Spezielle Gesetze und Anforderungen sind im jeweiligen Rechtskataster geregelt.

3.2 Bewusstsein für Informationssicherheit

Um Informationssicherheit gewährleisten zu können, sind angemessene technische und organisatorische Maßnahmen erforderlich. Diese können nur dann hinreichend wirksam sein, wenn alle Mitarbeiter die möglichen Gefährdungen für die Informationssicherheit kennen und in ihren Aufgabenbereichen entsprechend verantwortlich handeln. Regelmäßige Fortbildungen zur

Informationssicherheit unterstützen die Effektivität des Informationssicherheitsmanagements. Die Schulungen und Informationen erfolgen digital über eLearnings oder klassisch in Vor-Ort Schulungen. Die regelnden und informierenden Dokumente werden digital vollständig oder in adäquat zusammengefasster Form im Intranet zur Verfügung gestellt. Das einzuführende ISMS besitzt absichernde Prozesse bezüglich der nachfolgenden Abschnitte.

3.2.1 Vermeidung materieller Schäden

Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, die Veränderung von Daten oder den Ausfall einer IT-Anwendung oder eines Systems entstehen.

3.2.2 Wahrung von Persönlichkeitsrechten und Betriebsgeheimnissen

Vertraulichkeit und Integrität der für das KFZ-Büro wichtigen Informationen sind zu schützen, unabhängig davon, in welcher Form sie vorliegen. Auch im Umgang mit elektronischen Dokumenten und Informationen ist daher Geheimhaltungsanweisungen strikt Folge zu leisten.

3.2.3 Vermeidung von Ansehensverlust bzw. Imageschaden

Finanzielle Schäden und ein negatives Image für das KFZ-Büro müssen verhindert werden. Informationssicherheit vermeidet einen Ansehensverlust und Imageschaden des Unternehmens.

3.3 Kontinuierliche Verbesserung

Die Leitlinie zur Informationssicherheit und alle weiteren Richtlinien werden regelmäßig, hinsichtlich Aktualität und Wirksamkeit, geprüft.

Werden Schwachstellen in der Informationssicherheit identifiziert, so werden neue geeignete Maßnahmen entwickelt, auf ihre Integrationsfähigkeit in die Geschäftsabläufe untersucht und nach erfolgter Verifizierung in die Prozesse integriert.

Die Geschäftsführung unterstützt die ständige Verbesserung des Sicherheitsniveaus.

Alle Beschäftigten des KFZ-Büros sind angehalten, an der kontinuierlichen Verbesserung des Sicherheitsniveaus mitzuwirken und mögliche Schwachstellen oder Verbesserungen, z.B. durch Hinweise oder Verbesserungsvorschläge, an die entsprechenden Stellen weiterzuleiten.

3.4 Aktualisierung und Information

Diese Leitlinie ist mindestens jährlich auf Aktualität zu überprüfen. Die Überprüfung ist in Form einer neuen Revision zu belegen. Die Änderungen werden in den regelmäßigen Treffen des ISB mit dem Datenschutzbeauftragten (DSB) besprochen. Unterjährige Vorfälle zur Informationssicherheit, welche eine Anpassung des ISMS erforderlich machen, sind unmittelbar mit GF, ISB und DSB abzustimmen.

Jährlich wird ein Management-Report zur Wirksamkeit des ISMS erstellt und entsprechende Handlungsempfehlungen daraus abgeleitet.

4 Konsequenzen bei Nichtbeachtung des ISMS

Vorsätzliche oder grob fahrlässige Handlungen, die die Sicherheitsvorgaben verletzen, können finanzielle Verluste bedeuten, Mitarbeiter, Geschäftspartner und Kunden schädigen oder den Ruf des Unternehmens gefährden. Die Folgen von Zuwiderhandlungen erstrecken sich auf alle Bereiche des Informationssicherheitsmanagements. Bewusste Verstöße gegen verpflichtende Sicherheitsregeln können arbeitsrechtliche und unter Umständen auch strafrechtliche Konsequenzen haben und zu Regressforderungen führen.

5 Rahmenwerk des ISMS

Das Rahmenwerk eines Informationssicherheitsmanagementsystems (ISMS) gemäß TISAX® bildet einen entscheidenden Leitfaden für Unternehmen, die in der Automobilindustrie tätig sind. TISAX® definiert einen standardisierten Ansatz zur Bewertung und Zertifizierung der Informationssicherheit.

ID	Aufbau des ISMS
1	Richtlinien und Organisation des IS
2	Human Resources
3	Physical Security and Business Continuity
4	Identity and Access Management
5	IT Security / Cyber Security
6	Supplier Relationships
7	Compliance

6 Regelmäßige Überprüfung dieser Leitlinie

Diese Leitlinie wird mindestens einmal im Jahr auf Aktualität überprüft.

7 Bereitstellung dieser Leitlinie

Diese Leitlinie ist öffentlich und wird im Internet zur Verfügung gestellt.

Braunschweig, 28.06.2023



Marcel Guretzki

Geschäftsführer