# Leitlinie zur Informationssicherheit

## GMH Gruppe

## Dokumentenhistorie

| Version | Aktion | Datum | Name | Kommentar |
|---|---|---|---|---|
| 0.1 | Neu | 01.08.2023 | Anneke Knue | Initial Version |
| 0.2 | Entwurf | 18.10.2023 | Thorsten Kurz | Überarbeitung |
| 1.0 | Freigabe | 08.12.2023 | Mathias Hölscher, Dr. Deniz Özcan | Freigabe |
| 1.1 | Überarbeitung | 08.01.2024 | Treubrodt / Grühn | Abgleich mit 1.1.1 Richtlinie |
| 1.2 | Q-Prüfung | 10.01.2024 | Treubrodt-Team | Abgleich mit 1.1.1 Richtlinie |
| 1.3 | Überarbeitung | 16.01.2024 | Anneke Knue | Abschnitt zur GMH angepasst |
| 2.0 | Freigabe | 23.01.2024 | Mathias Hölscher, Dr. Deniz Özcan | Freigabe |
| | | | | |
| | | | | |

## Dokumentenfreigabe

| Rolle | Name | Abteilung | Datum |
|---|---|---|---|
| Autoren | Knue | IT-Management | 01.08.2023 |
| Reviewer | Kurz | Qualitätsmanagement | 18.10.2023 |
| Genehmiger | Hölscher, Özcan | CFO, Director CC-IT | 23.01.2024 |

# Inhalt

## Abbildungsverzeichnis



## Tabellenverzeichnis



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

# 1 Einleitung

Durch vorsätzlich schadhafte Handlungen, menschliche Fehlhandlungen, einen Ausfall der Informationstechnik oder Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität von Informationen kann die Existenz der GMH Gruppe gefährdet werden. Um Reputations- oder finanziellen Schäden entgegenzuwirken, soll die Informationssicherheit in der GMH Gruppe dauerhaft aufgebaut, verwirklicht, aufrechterhalten und fortlaufend verbessert werden. Hierzu ist ein Informationssicherheitsmanagement etabliert, damit die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit in Bezug auf die Informationen gewährleistet werden können. Ebenfalls soll ein einheitliches Verständnis zur Informationssicherheit in der GMH Gruppe vorliegen.

## 1.1 Die GMH Gruppe

Die GMH Gruppe zählt zu den größten privat geführten metallverarbeitenden Unternehmensgruppen in Europa und umfasst insgesamt 20 mittelständische Produktionsunternehmen in den Bereichen Stahl, Schmiede und Guss mit rund 6.000 Mitarbeitern. Ihre breitgefächerten Produkte und Dienstleistungen finden Anwendung in verschiedenen Industriezweigen, darunter Automotive, Bahntechnik, Energieerzeugung, Transport, Logistik, Aerospace, Land- und Baumaschinen sowie im Allgemeinen Maschinen- und Anlagenbau. Über der gesamten Gruppe steht die Georgsmarienhütte Holding GmbH als Mutterkonzern, die die gesamte GMH Gruppe koordiniert.

## 1.2 Geltungsbereich

Die Leitlinie zur Informationssicherheit gilt für alle Mitarbeiter der GMH Gruppe.

Diese Leitlinie zur Informationssicherheit erstreckt sich auf alle Informationen, die von oder mit IT-Systemen und nicht IT-Systemen verarbeitet werden. An den einzelnen Standorten können darüber hinaus weitere Richtlinien und Regelungen gelten, die in diesen Fällen lediglich die Standorte selbst, also den Anwendungsbereich betreffen.

**Alle zentralen Themen sind entsprechend mit dem GMH Gruppe Logo gekennzeichnet. Sofern es sich um dezentrale Themen handelt, sind diese mit dem standortspezifischen Logo versehen.**

## 1.3 Ansprechpartner

Ansprechpartner zu allen Fragen dieser Leitlinie ist der Informationssicherheitsmanager (ISM), welcher im Competence Center IT der GMH Gruppe angesiedelt und im Auftrag, der nach TISAX zu zertifizierenden Standorte der GMH Gruppe tätig ist.

An den einzelnen Standorten, die nach TISAX zertifiziert werden, sind Informationssicherheitskoordinatoren (ISK) Ansprechpartner für Mitarbeiter. Diese ISK berichten an den ISM der Gruppe.

### 1.4 Verantwortlichkeiten

Diese Leitlinie hat die Geschäftsführung der Georgsmarienhütte Holding GmbH genehmigt und freigegeben. Die Beachtung, Verteilung und Umsetzung dieser Leitlinie in den Gruppenunternehmen obliegt der Verantwortung der jeweiligen Geschäftsführungen der nach TISAX zu zertifizierenden Standorte. Diese sind den jeweiligen Gruppen-Homepages zu entnehmen.

## 2 Stellenwert der Informationstechnologie (IT) und Informationssicherheit

Die Informationssicherheit sowie Informationstechnologie (IT) hat in der GMH Gruppe einen sehr hohen Stellenwert und stellt ein wichtiges Qualitätsmerkmal der Datenverarbeitung dar, da viele wesentliche strategische und operative Geschäftsprozesse in der GMH Gruppe durch Informationstechnologien maßgeblich unterstützt werden.

Ziel der GMH Gruppe ist es, die Daten und IT-Systeme in dem jeweiligen Unternehmen über alle Geschäftsprozesse in ihrer Verfügbarkeit so zu sichern, dass die Integrität und Vertraulichkeit von sensiblen Unternehmensdaten 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 der Georgsmarienhütte Holding GmbH hat entschieden, dass ein angemessenes Sicherheitsniveau für einen 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) für die GMH Gruppenunternehmen mit Automotivbezug,
- die Zertifizierung der Gruppenunternehmen mit direkter oder indirekter Zulieferung an die Automotiv-Industrie,
- 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 der GMH Gruppe eingehalten werden. Die gruppenweiten Gesetze sind nachfolgend geregelt:

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

Spezielle Gesetze und Anforderungen der einzelnen Gruppenunternehmen 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.

## 3.3 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.

## 3.4 Wahrung von Persönlichkeitsrechten und Betriebsgeheimnissen

Vertraulichkeit und Integrität der für die GMH Gruppe 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.

## 3.5 Vermeidung von Ansehensverlust bzw. Imageschaden

Finanzielle Schäden und ein negatives Image für die GMH Gruppe müssen verhindert werden. Informationssicherheit vermeidet einen Ansehensverlust und Imageschaden des Unternehmens.

### 3.6 Kontinuierliche Verbesserung

Die GMH Gruppe strebt eine kontinuierliche Verbesserung ihrer Prozesse rund um die Informationssicherheit an. Die Gruppenunternehmen müssen für den kontinuierlichen Verbesserungsprozess des ISMS einen risikobasierten Ansatz betrachten und umsetzen. Die Verbesserungsaktivitäten sind interdisziplinär anhand der etablierten Prozesse im jeweiligen Gruppenunternehmen in Form von objektiven Nachweisen zu belegen. Die Ergebnisse sind zudem im Risikomanagement zu berücksichtigen. Des Weiteren erfolgt ein regelmäßiger Erfahrungsaustausch zwischen dem Informationssicherheitsmanager und den Informationssicherheitskoordinatoren.

### 3.7 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 Informationssicherheitsmanagers (ISM) mit den Informationssicherheitskoordinatoren (ISK) besprochen. Unterjährige Vorfälle zur Informationssicherheit, welche eine Anpassung des ISMS erforderlich machen, sind unmittelbar mit dem ISM abzustimmen. Dieser sorgt für die Informationsweitergabe an die Informationskoordinatoren.

Die Geschäftsführungen werden regelmäßig, halbjährlich über die Risiken und Chancen hinsichtlich des ISMS durch das CC Risk and Insurance informiert. Des Weiteren hat der ISK ein jährliches Managementreview mit seiner Geschäftsführung, synchron zu dem ISM mit der Geschäftsführung der Holding, durchzuführen und zu dokumentieren.

Die Änderungen an der Struktur und den Anforderungen des ISMS sind gemäß den etablierten Prozessen des jeweiligen Unternehmens zu schulen bzw. zu informieren.

## 4 Organisation des Informationssicherheitsmanagements

Die Gesamtverantwortung für die Informationssicherheit obliegt dem obersten Management (strategische Ebene). Um dieser Verantwortung gerecht zu werden und die unterschiedlichen Aufgaben und Pflichten, die aus der Informationssicherheit erwachsen, angemessen umzusetzen, ist eine mehrstufige Sicherheitsstruktur eingerichtet worden. Die verantwortlichen Mitarbeiter sind benannt und für ihre Aufgaben entsprechend qualifiziert.

Zur Vermeidung von Interessenkonflikten sind die aufgeführten Verantwortlichkeiten organisatorisch getrennt (Funktionstrennung, Separation of Duties):

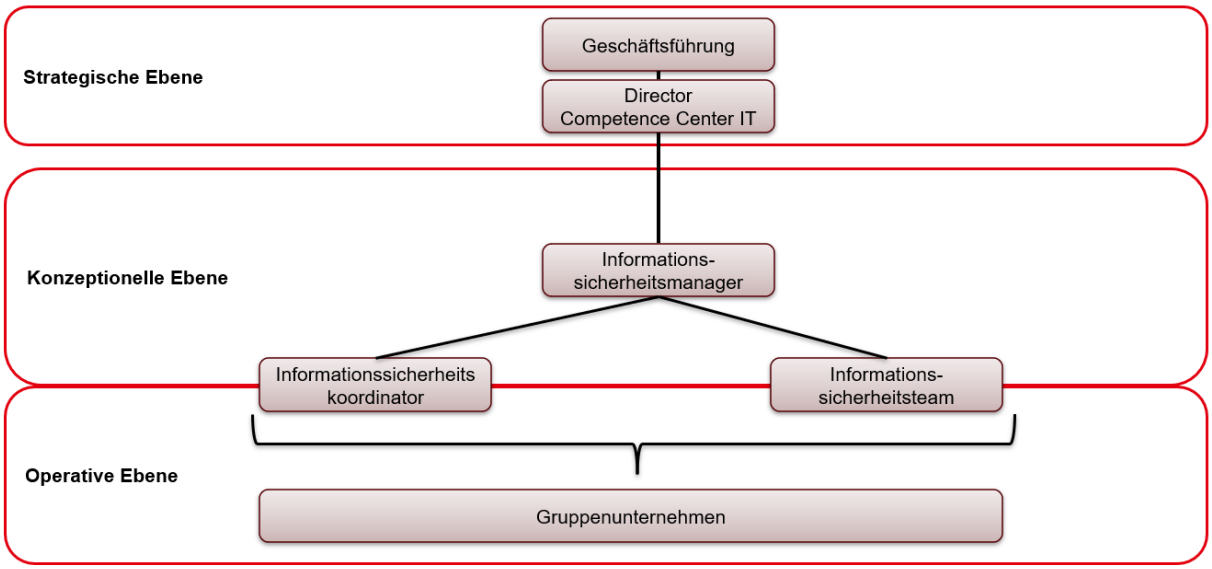


**Abbildung 1 Aufbauorganisation Informationssicherheit GMH Gruppe**

## 4.1 Strategische Ebene

### 4.1.1 Geschäftsführung der Holding

Die Geschäftsführung trägt die Gesamtverantwortung, dass ein ISMS in den Gruppenunternehmen etabliert, erhalten und weiterentwickelt wird. Für die Umsetzung des ISMS im jeweiligen Unternehmen ist die Geschäftsführung des jeweiligen Standortes verantwortlich. Die dafür technischen und personellen Bereitstellungen von Ressourcen für die Umsetzung der Informationssicherheit und deren angemessene Einbettung in die Strukturen und die Hierarchie des Unternehmens obliegt dem Unternehmen. Zusätzlich fungiert sie als Vorbildfunktion (Tone from the Top).

### 4.1.2 Director Competence Center IT

Der Director Competence Center (CC) IT ist für die Steuerung der IT in der GMH Gruppe zuständig. Er ist der Geschäftsführung der Georgsmarienhütte Holding GmbH unterstellt und setzt die Anforderung zur IT-Sicherheit durch angemessene Schutzmaßnahmen um. Zur Erfüllung dieser Aufgabe bedient er sich an den Mitarbeitern der IT-Organisation.

## 4.2 Konzeptionelle Ebene

### 4.2.1 Informationssicherheitsmanager

Der Informationssicherheitsmanager ist von der Geschäftsführung der Georgsmarienhütte Holding GmbH bestellt worden. Er steht der strategischen Ebene in den folgenden Tätigkeiten unterstützend zur Verfügung:

- Sicherheitsprozess zu steuern und zu koordinieren,
- die strategische Ebene bei der Erstellung der Sicherheitsleitlinie zu unterstützen,

- die Erstellung des Sicherheitskonzepts und zugehöriger Teilkonzepte und übergreifender Richtlinien zu koordinieren,
- Realisierungspläne für Sicherheitsmaßnahmen anzufertigen sowie ihre Umsetzung zu initiieren und zu überprüfen,
- der strategischen Ebene und anderen Sicherheitsverantwortlichen über den Status der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- sicherheitsrelevante Vorfälle zu untersuchen sowie
- Sensibilisierungen und Schulungen zur Informationssicherheit zu initiieren und zu koordinieren.

### 4.2.2 Informationssicherheitskoordinator je Standort

Der Informationssicherheitskoordinator wird je Standort benannt. Er arbeitet eng mit dem Informationssicherheitsmanager zusammen und stimmt sich in regelmäßigen Abständen ab. Er koordiniert die Informationssicherheitsvorgaben und -prozesse am Standort und überwacht deren Einhaltung.

### 4.2.3 Informationssicherheitsteam

Das gesamte Informationssicherheitsteam (kurz ISMS-Team) setzt sich aus der strategischen Ebene, der konzeptionellen Ebene und der operativen Ebene zusammen (Abbildung 2).

Das Team legt Maßnahmen fest, die aus fachlicher Sicht zur Verbesserung und Erhaltung der Informationssicherheit ergriffen werden müssen. Sie unterstützen den ISM und den ISK bei der Wahrnehmung seiner Aufgaben:

- bei der Definition der Sicherheitsziele und -strategien,
- bei der Entwicklung der Sicherheitsleitlinie und Prüfung ihrer Umsetzung,
- bei der Erstellung des Sicherheitskonzepts,
- bei der Initiierung, Steuerung und Überwachung des Sicherheitsprozesses,
- bei der Konzeption von Schulungs- und Sensibilisierungsprogrammen,
- bei der Beratung der Fachverantwortlichen, den IT-Betrieb.

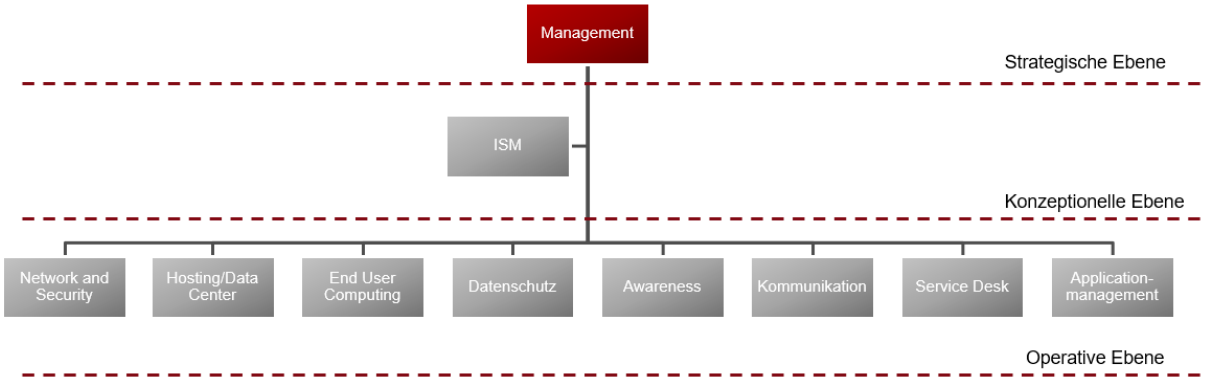


**Abbildung 2 Aufbau ISMS-Team**

## 4.3 Operative Ebene

Die Operative Ebene setzt sich aus den fachlichen IT-Verantwortlichen an den jeweiligen Standorten des Competence Center IT zusammen, die für die Umsetzung der Sicherheitsmaßnahmen zum Schutz der Informationen verantwortlich sind (vgl. Abbildung 2) sowie den Mitarbeitern. Das Competence Center IT wird durch das ISMS-Team sowie den ISK unterstützt. Alle Mitarbeiter innerhalb der GMH Gruppe sind innerhalb ihres zugewiesenen Bereichs dafür verantwortlich, dass durch wirksame Maßnahmen die Informationssicherheitsziele realisiert und umgesetzt werden. Zur Verbesserung der Informationssicherheit haben alle Mitarbeiter des jeweiligen Unternehmens mit dem jeweiligen Datenschutzbeauftragten, IT-Verantwortlichen und auch mit dem ISMS-Team zu kooperieren.

## 4.4 Wirkrichtung innerhalb des ISMS

Innerhalb des ISMS gilt die Top-Down und Bottom-up Planung, d.h. die einzelnen Teilbereiche arbeiten in Eigenverantwortung entsprechende Ergebnisse aus, die im Zuge der Gesamtplanung miteinander verknüpft und koordiniert werden. Dies kann entweder von der strategischen Ebene nach unten zur operativen Ebene oder umgekehrt von der operativen Ebene hoch zur strategischen Ebene erfolgen.

# 5 Aufbau der Informationssicherheitsdokumentation

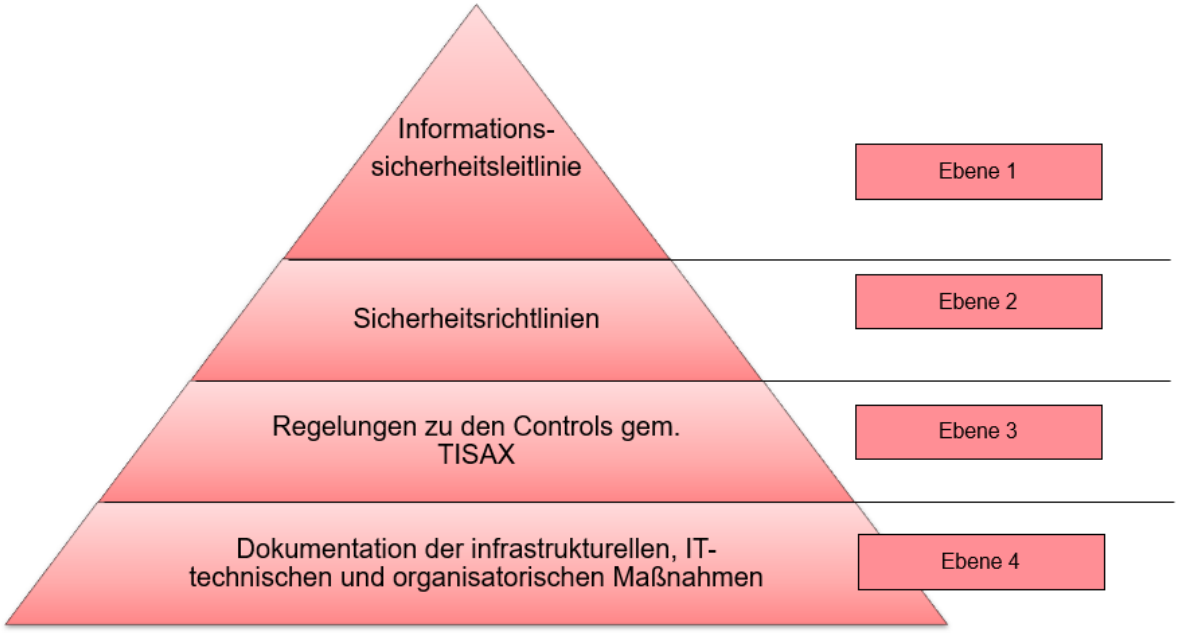


**Abbildung 3 Aufbau der Informationssicherheitsdokumentation**

Die Lenkung der Dokumente unterliegt den Anforderungen der VDA-ISA.

# 6 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.

# 7 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 | Informationssicherheitsrichtlinien und das Unternehmen |
| 2 | Human Ressources |
| 3 | Physical Security and Business Continuity |
| 4 | Identity and Access Management |
| 5 | IT Security / Cyber Security |
| 6 | Supplier Relationships |
| 7 | Compliance |

**Tabelle 1 Aufbau des ISMS**

# 8 Regelmäßige Überprüfung dieser Leitlinie

Diese Leitlinie wird mindestens einmal im Jahr vom ISMS-Team auf Aktualität überprüft.

# 9 Bereitstellung dieser Leitlinie

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

Georgsmarienhütte, 23.01.2024

Mathias Hölscher
24.01.2024 20:11:05 [UTC+1]

**Mathias Hölscher**
Geschäftsführung Georgsmarienhütte Holding GmbH

Deniz Oezcan
23.01.2024 18:05:17 [UTC+1]

**Dr. Deniz Özcan**
Director Competence Center IT