Informationssicherheits-Managementsystem

Toyota Deutschland GmbH

Informationssicherheitsleitlinie

Inhaltsverzeichnis

Inhaltsverzeichnis **2**

1 Präambel **3**

2 Allgemeines **4**

2.1 Ziele 4

2.2 Geltungsbereich und interessierte Parteien 4

2.3 Klimawandel 6

2.4 Normbezug 6

2.5 Leitlinienverantwortung 6

3 Informationssicherheitsstrategie **7**

4 Sicherheitsbewusstsein **8**

5 Grundsätze der Informationssicherheit **9**

5.1 Sicherheit als integraler Bestandteil 9

5.2 Einhaltung vertraglicher und sonstiger verbindlicher Anforderungen 9

5.3 Schutz von Daten und Ressourcen 9

5.4 Gewährleistung der Nachvollziehbarkeit 9

5.5 Gewährleistung der Wirtschaftlichkeit 9

5.6 Aufrechterhaltung des sicheren Geschäftsbetriebs 10

5.7 Informationssicherheit in Projekten 10

6 Detailziele **11**

7 Verantwortlichkeiten **12**

7.1 Geschäftsleitung 12

7.2 Chief Information Security Officer 12

7.3 Information Security Officer 12

7.4 Betrieblicher Datenschutzbeauftragter 12

7.5 Anwendungsnutzer 13

8 Verbesserung der Informationssicherheit **14**

9 Durchsetzung der Informationssicherheitsleitlinie **15**

10 Erklärung der Geschäftsleitung **16**

1 Präambel

Die Entwicklung und der Betrieb von Informations- und Kommunikationstechnik ist von einem stetig steigenden Integrations-, Vernetzungs- und Verteilungsgrad gekennzeichnet.

Durch die vermehrte Nutzung der Informations- und Kommunikationstechnik und deren Einbindung in die tägliche Arbeit steigt die Abhängigkeit aller Unternehmen der Toyota Deutschland GmbH von dieser Technik.

Ein wesentlicher und bestimmender Faktor der Informationssicherheit ist – neben dem Verhalten von Menschen – auch die Fähigkeit einer Organisation, mit den vorhandenen Mitteln und technischen Möglichkeiten adäquat umzugehen. Sicherheitsrisiken müssen rechtzeitig erkannt werden, damit angemessene Maßnahmen zur Gewährleistung der Informationssicherheit konsequent umgesetzt werden können.

Vor diesem Hintergrund betreibt die Toyota Deutschland GmbH ein entsprechendes Informationssicherheitsmanagementsystem (ISMS).

Die Geschäftsleitung der Toyota Deutschland GmbH verabschiedet diese Leitlinie zur Informationssicherheit als zentralen Bestandteil des ISMS.

2 Allgemeines

2.1 Ziele

Die Toyota Deutschland GmbH sieht sich in der Verpflichtung zur Gewährleistung von Informationssicherheit. Der IT-Einsatz ist von existentieller Bedeutung und unterliegt ständiger Dynamisierung, die stetig neue Herausforderungen mit sich bringt und neue Lösungen erfordert. Das Umfeld ist geprägt von steigenden Anforderungen an Sicherheit, Leistungsfähigkeit und Flexibilität, häufig einhergehend mit einer steigenden Komplexität.

Der zunehmende Einsatz und das Zusammenwachsen von Informationsverarbeitungssystemen und Kommunikationstechnologien erfordern zunehmend Anstrengungen zum Schutz der von der Toyota Deutschland GmbH bearbeiteten und gespeicherten Daten. Der Verfügbarkeit unserer IT-Systeme sowie dem sicheren Umgang mit unseren Unternehmensdaten kommen hierbei eine besondere Bedeutung zu.

Das wachsende Sicherheitsbewusstsein in der Öffentlichkeit und damit einhergehende neue gesetzliche Rahmenbedingungen erfordern unser aktives Handeln. Die zunehmende Notwendigkeit unseres Informationsangebotes gegenüber Kunden, Interessenten und Partnern sowie die verstärkte Nutzung von Cloud-Services sind weitere Herausforderungen.

Zum Schutz der Toyota Deutschland GmbH, deren Geschäftspartnern und Kunden sind Informationen vor Missbrauch und Verlust von Integrität, Vertraulichkeit, Verfügbarkeit und/oder Resilienz zu bewahren.

2.2 Geltungsbereich und interessierte Parteien

Die Toyota Deutschland GmbH betreibt Handel mit Automobilen sowie Ersatzteilen und Zubehör aller Art, insbesondere den Import und Vertrieb von Automobilen und anderen Erzeugnissen des Herstellers Toyota Motor Co., Ltd. aus Toyota City in Japan.

Die vorliegende Informationssicherheitsleitlinie gilt für alle Mitarbeiterinnen und Mitarbeiter der Toyota Deutschland GmbH. Sie umfasst alle eingesetzten Soft- und Hardwarekomponenten sowie die gesamte Infrastruktur der Toyota Deutschland GmbH und die damit verbundenen Prozesse. Dies schließt auch die von anderen Organisationseinheiten betriebenen und für die Toyota Deutschland GmbH bereitgestellten Anwendungen, IT-Komponenten und Infrastrukturen ein.

Die Leitlinie soll das Bewusstsein aller Nutzerinnen und Nutzer von Informationstechnologie schärfen. Sie sollen sich der Bedeutung der Informationssicherheit bewusst sein, aktiv zur Vermeidung und Bekämpfung von Schäden beitragen, verantwortungsvoll mit den Informationssystemen sowie den darin gespeicherten Daten umgehen.

Neben den konzerneigenen Unternehmen und Organisationseinheiten sind unsere Kunden, Interessenten und Geschäftspartner die primären interessierten Parteien. Auch die Öffentlichkeit selbst zählen wir dazu – dies ist allein schon unserer Verpflichtung gegenüber unseren Mitbürgerinnen und Mitbürgern, unserer Umwelt und der Zukunft nachfolgender Generationen geschuldet.

Anforderungen dieser bzw. weiterer interessierter Parteien wurden mit Blick auf die Informationssicherheit identifiziert und sind in der nachfolgenden Tabelle beschrieben.

Interessierte Partei	Bedürfnisse/Erwartungen	Maßnahmen
Gewerkschaft und Betriebsrat	Angemessene Arbeitsbedingungen, Sicherheit der Mitarbeiterdaten, Transparenz, Weiterbildung, Mitbestimmung, Rechtskonformität	Hochwertige Arbeitsgeräte, Sicherheitsausrüstung, Verschlüsselung, Zugangs- und Zutrittsbeschränkungen, transparente Kommunikation, Schulungen, Feedback, Audits, Compliance-Prüfungen
Mitarbeiterinnen und Mitarbeiter	Sicherheit der Mitarbeiterdaten, Verlässlichkeit, Reputation, Arbeitsbedingungen, Nachhaltigkeit und Ressourcenschonung	Schulungen, Arbeits- und Tarifverträge, Richtlinien, Zugangs- und Zutrittsbeschränkungen, Verschlüsselung, Nachhaltigkeitsstrategien
Kundinnen und Kunden	Sicherheit der Kundendaten, Zurechenbarkeit, Vertraulichkeit, Integrität, Verbindlichkeit, Nachhaltigkeit	Schulungen, Richtlinien, Zugangs- und Zutrittsbeschränkungen, Verschlüsselung, Datenschutzvereinbarungen, Nachhaltigkeitsstrategien
Händler	Sicherheit der Händlerdaten, Zurechenbarkeit, Integrität, Vertraulichkeit, Verfügbarkeit, Verbindlichkeit, Reputation	Schulungen, Richtlinien, Zugangs- und Zutrittsbeschränkungen, Verschlüsselung, Service- und Vertraulichkeitsvereinbarungen, Nachhaltigkeitsstrategien
Hersteller, Lieferanten, Dienstleister	Zurechenbarkeit, Integrität, Vertraulichkeit, Nachhaltigkeit und Ressourcenschonung	Zugangs- und Zutrittsbeschränkungen, Audits, Verschlüsselung, Service- und Vertraulichkeitsvereinbarungen, Nachhaltigkeitsstrategien
Aktionäre und Investoren	Erhalt bzw. Steigerung des Wertes der Toyota Deutschland GmbH, Verlässlichkeit, Nachhaltigkeit	Transparente Berichtserstattung, Audits, Nachhaltigkeitsstrategien
Aufsichtsbehörden	Gesetzeskonformität, Verfügbarkeit, Zurechenbarkeit, Verbindlichkeit, Einhaltung von Meldepflichten	Compliance-Prüfungen, Berichterstattung, Audits, Meldeprozesse
Branchenverbände (VDIK, THLV)	Integrität, Reputation, Verbindlichkeit, Einhaltung branchenspezifischer Anforderungen und Standards	Transparente Berichterstattung
Öffentlichkeit/Medien	Verlässlichkeit (Sicherung der Arbeitsplätze, Attraktivität des Standortes), Reputation, Transparenz, Nachhaltigkeit und Ressourcenschonung	Pressemitteilungen und Updates, Nachhaltigkeitsstrategien

2-1 Interessierte Parteien (Auszug)

2.3 Klimawandel

Die Betrachtung des Klimawandels fördert ein verantwortungsbewusstes Verhalten gegenüber dessen Entwicklung, Fortschreitung und Veränderung. Dieses Augenmerk ist einer der Treiber für eine kontinuierliche Verbesserung der Sicherheitsmaßnahmen der Toyota Deutschland GmbH. Hier wird auf das Bewusstsein und das Engagement aller Mitarbeiterinnen und Mitarbeiter gesetzt, um das ISMS auch in Zeiten klimatischer Veränderungen robust und widerstandsfähig zu gestalten.

Dazu müssen die Verantwortung und das Bewusstsein jedes Einzelnen gestärkt werden.

Unsere Mitarbeiterinnen und Mitarbeiter sind sich über klimabezogene Risiken – wie Extremwetter oder Energieausfälle – bewusst. Solche Risiken können das ISMS an sich ebenso wie die Aufgaben der Mitarbeiterinnen und Mitarbeiter im Umfeld ihrer täglichen Arbeit beeinflussen. Dabei ist es erwünscht, dass sie klimabedingte Gefährdungen erkennen und melden. So ist auch ein verantwortungsvoller Umgang mit der IT-Infrastruktur ein zu betrachtender Aspekt. Die Mitarbeiterinnen und Mitarbeiter sind angehalten, nachhaltig mit IT- und Kommunikationssystemen umzugehen und so die Lebensdauer der Geräte zu maximieren. Außerdem sind sie eingeladen, Vorschläge zur Verbesserung klimabezogener Sicherheitsmaßnahmen einzureichen, um das ISMS an aktuelle Herausforderungen des Klimawandels anzupassen.

2.4 Normbezug

Diese Dokumentation bezieht sich auf folgende Norm:

- DIN EN ISO 27001:2022

2.5 Leitlinienverantwortung

Die Leitlinienverantwortung liegt innerhalb der Toyota Deutschland GmbH beim Information Security Officer der Toyota Deutschland GmbH.

3 Informationssicherheitsstrategie

Kerninhalte der Informationssicherheitsstrategie sind der Schutz von Informationen vor unberechtigter Offenlegung, vor Spionage, vor Modifikationen, Einfügungen, Löschungen und Umordnungen sowie die Gewährleistung, dass Informationen für berechtigte User möglichst jederzeit verfügbar sind.

Das ISMS umfasst die Einrichtung, die Implementierung, den Betrieb, die Überwachung, die Wartung und die Verbesserung der Informationssicherheit und stützt sich dabei wesentlich auf das Management von Geschäftsrisiken.

Zum ISMS gehört auch ein kontinuierlicher Verbesserungsprozess, der über Revisionen (interne und externe Audits) die Wirksamkeit des Managementsystems beurteilt und dadurch zu einer stringenten Anpassung und Aktualisierung des ISMS führt.

4 Sicherheitsbewusstsein

Die Informationssicherheit ist ein zunehmend wichtiger Faktor für die Wettbewerbsfähigkeit der Toyota Deutschland GmbH geworden. Daraus folgt, dass das Sicherheitsbewusstsein einer der entscheidenden Erfolgsfaktoren ist.

Sicherheitsbewusstsein ist durch folgendes Verhalten aller Mitarbeiterinnen und Mitarbeiter gekennzeichnet:

- Erkennen, dass effektive Sicherheit ein kritisches und wesentliches Element der Unternehmensphilosophie ist.
- Berücksichtigen und Einbringen des eigenen Sicherheitsbewusstseins bei allen täglich anfallenden Aktivitäten.
- Übernahme persönlicher Verantwortung für proaktive Maßnahmen in Bezug auf sämtliche Risiken für Mitarbeiterinnen und Mitarbeiter, Informationen, Vermögenswerte und die Fortführung der Geschäftstätigkeit bei eventuell auftretenden Störungen bzw. Notfällen.
- Lesen und Verstehen von Richtlinien. Hierzu können Mitarbeiterinnen und Mitarbeiter bei möglichen Fragen zu den Richtlinien den Information Security Officer der Toyota Deutschland GmbH kontaktieren.

5 Grundsätze der Informationssicherheit

5.1 Sicherheit als integraler Bestandteil

Die Informationssicherheitsleitlinie ist – neben weiteren Grundsätzen der Unternehmenssicherheit, wie z. B. den Themen Gebäudesicherheit, Personalsicherheit, Versicherungsschutz, Sicherheit und Recht – ein integraler Bestandteil der Geschäftspolitik und bedarf der gesamtheitlichen Betrachtung.

Eine nicht oder nicht konsequent durchgeführte Umsetzung der Informationssicherheitsleitlinie kann Vermögens- und sonstige Schäden nach sich ziehen, deren Ausmaße nicht absehbar sind.

5.2 Einhaltung vertraglicher und sonstiger verbindlicher Anforderungen

Die Einhaltung aller relevanten vertraglichen und sonstigen Anforderungen ist unabdingbar. Sie entspricht dem Selbstverständnis der Toyota Deutschland GmbH und ihrer Unternehmen und verringert gleichzeitig die Gefahr von Rechtsverletzungen.

Die Erfüllung der vertraglichen und sonstigen verbindlichen Anforderungen mündet in die Notwendigkeit der Anpassung der geltenden arbeitsordnenden Regelungen im Unternehmen.

5.3 Schutz von Daten und Ressourcen

Die Toyota Deutschland GmbH schützt alle relevanten unternehmenseigenen und ihr anvertrauten Daten und Ressourcen dergestalt, dass die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Resilienz stets und im Einklang mit Gesetzen, Vorschriften und bestehenden vertraglichen Verpflichtungen gewährleistet werden.

Hierzu gehört auch die Sicherstellung einer datenschutzrechtlich ordnungsgemäßen Verarbeitung personenbezogener Daten.

5.4 Gewährleistung der Nachvollziehbarkeit

Die Nachvollziehbarkeit sicherheitsrelevanter Aktivitäten ist eine unabdingbare Forderung, sowohl aus entsprechenden gesetzlichen und regulatorischen als auch aus geschäftlichen Anforderungen an die Toyota Deutschland GmbH. Daher werden sicherheitsrelevante Aktivitäten protokolliert.

5.5 Gewährleistung der Wirtschaftlichkeit

Die Wirtschaftlichkeit aller einzusetzenden Sicherheitsmaßnahmen zur Aufrechterhaltung eines sicheren IT-Betriebs ist unbedingt zu gewährleisten. Ohne Einbeziehung von Wirtschaftlichkeitsaspekten bei der Auswahl von operativen Komponenten bzw. bei der Entscheidung zu Sicherheitseinrichtungen besteht die Gefahr der Überdimensionierung von Systemen. Im Extremfall können Aufwände und Kosten bei Nichtbeachtung dieses Punktes dauerhaft höher liegen als der Schaden, der entstünde, wenn die korrespondierenden Risiken schlagend werden würden.

5.6 Aufrechterhaltung des sicheren Geschäftsbetriebs

Im Informationssicherheitsprozess geht es nicht nur darum, das angestrebte Informationssicherheitsniveau zu erreichen, sondern dieses auch dauerhaft zu gewährleisten. Dazu gehören im Wesentlichen:

- Reaktion auf Gesetzesänderungen und vertragliche Verpflichtungen,
- sichere Inbetriebnahme neuer Hard- und Software,
- kontinuierliche Verbesserung der Sicherheit bestehender Systeme,
- kontinuierlicher Betrieb des Asset- und des Risiko-Managements,
- Reaktion auf Änderung von Geschäftsprozessen und/oder Organisationsstrukturen,
- Prüfung, ob vorhandene Maßnahmen noch hinreichend sind.

Änderungen am ISMS, die aus den oben genannten Punkten folgen, müssen vollumfänglich integriert und kommuniziert werden.

Eine regelmäßige Untersuchung des Informationssicherheitsprozesses wird vom Information Security Officer der Toyota Deutschland GmbH initiiert.

5.7 Informationssicherheit in Projekten

In Projekten ist sicherzustellen, dass der Information Security Officer frühzeitig mit einbezogen wird. Er kann Hinweise und Vorgaben zur Informationssicherheit geben und, falls notwendig, interne/externe Prüfungen veranlassen. Die Umsetzung der Maßnahmen wird durch ihn nicht nur im laufenden Projektbetrieb, sondern insbesondere vor dem Abschluss des Projektes geprüft und verifiziert.

Der Information Security Officer entscheidet, ggf. in Abstimmung mit dem Chief Information Security Officer, ob eine Informationssicherheitsrelevanz im jeweiligen Projekt gegeben und damit eine durchgängige Projektbegleitung durch ihn erforderlich ist.

6 Detailziele

Die Bereitstellung funktionsfähiger Informationssysteme im Geltungsbereich des ISMS ist geprägt durch den sicherheitsbewussten Umgang mit sämtlichen Systemen. Dieser sensible Umgang mit ISMS-relevanten Aufgabenkreisen ist eine wesentliche Voraussetzung für die Einhaltung der Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Resilienz.

Sämtliche IT-Prozesse im Geltungsbereich des ISMS sind so zu betreiben, dass durch wirksame Informationssicherheitsmaßnahmen eine korrekte und nachvollziehbare Bearbeitung der Informationen und der daraus abgeleiteten Ergebnisse – so weit als möglich – unterstützt wird. Ziele hierbei sind:

- die Gewährleistung der vollumfänglichen Umsetzung der aus den gesetzlichen Vorgaben resultierenden Anforderungen an die Informationssicherheit,
- eine umfassende Vermeidung, Verhinderung oder zumindest eine Reduzierung materieller und immaterieller Schäden,
- die kontinuierliche Verbesserung des ISMS.

Das ISMS ist als qualitätssichernde Methodik unter Berücksichtigung sicherheitsrelevanter Aspekte der Norm ISO 27001 zu verstehen. Dies gilt sowohl bei Bereitstellung und Betrieb der geltungsbereichsbezogenen IT sowie der darauf gespeicherten und genutzten Daten als auch beim IS-relevanten Selbstverständnis der Mitarbeiterinnen, Mitarbeiter und sonstigen Beschäftigten der Toyota Deutschland GmbH. Dazu muss das ISMS angemessen in die bestehende Organisation und deren Geschäftsprozesse integriert werden. Auch unternehmerische Anforderungen müssen berücksichtigt und in ihrer Gesamtheit – vor allem unter wirtschaftlichen Gesichtspunkten – betrachtet werden.

Folgenden Informationssicherheitszielen und Informationssicherheitsmaßnahmen ist hierbei besondere Beachtung zu schenken:

- Kontinuierliche Durchführung und wirksame Implementierung des informationssicherheitsspezifischen Risikomanagements,
- Übereinstimmung der Zielsetzungen des ISMS mit den übergeordneten Zielsetzungen und der Strategie der Toyota Deutschland GmbH,
- Einführung von Key Performance Indikatoren (KPI) zur Messung der Erreichung dieser Ziele, einschließlich Messung und Dokumentation der KPI und deren Werte in den Aufzeichnungen zum Management Review.

7 Verantwortlichkeiten

7.1 Geschäftsleitung

Die Verantwortung für die Einhaltung aller Bestimmungen zur Informationssicherheit liegt bei der Geschäftsleitung der Toyota Deutschland GmbH.

Die Geschäftsleitung sorgt dafür, dass die zum Betrieb des ISMS erforderlichen Ressourcen bereitstehen. Dies betrifft insbesondere folgende Punkte:

- Qualifiziertes Personal in ausreichendem Umfang,
- Technik zur Unterstützung des ISMS,
- Mittel zur Maßnahmenumsetzung.

7.2 Chief Information Security Officer

Der Chief Information Security Officer ist das Bindeglied zwischen den Bereichen Informationstechnik, Informationssicherheit und dem eigentlichen Geschäftsbetrieb der Toyota Deutschland GmbH. Er erarbeitet die Informationssicherheits-Strategie auf Basis der bzw. in Übereinstimmung mit den Geschäftszielen – Fokus ist das Erreichen des notwendigen Schutzniveaus, ohne die Flexibilität und Beweglichkeit der Geschäftsprozesse einzuschränken.

Der Chief Information Security Officer nimmt im Rahmen seiner Funktion eine Führungsrolle in der Toyota Deutschland GmbH ein und gibt die grundsätzliche bzw. strategische Richtung für das Sicherheitsteam vor. Er gibt Empfehlungen auf Grundlage der aktuellen Erkenntnisse im Umfeld der Informations- bzw. Cybersicherheit ab, um auch aktuelle Bedrohungen abwehren zu können.

7.3 Information Security Officer

Der Information Security Officer besitzt eine unabhängige und organisatorisch herausgehobene Stellung. Er ist zuständig für alle Belange der Informationssicherheit innerhalb der Toyota Deutschland GmbH und unterstützt die Leitungsebene bei deren Aufgaben bezüglich der Informationssicherheit.

Er ist in dieser Rolle dem Chief Information Security Officer unterstellt und berichtet direkt an diesen.

7.4 Betrieblicher Datenschutzbeauftragter

Für die unternehmensweite Überwachung einer datenschutzrechtlich ordnungsgemäßen Verarbeitung personenbezogener Daten ist der betriebliche Datenschutzbeauftragte der Toyota Deutschland GmbH verantwortlich, soweit gesetzliche oder behördliche Vorgaben bezüglich des Datenschutzes betroffen sind. Er arbeitet mit den jeweiligen Ansprechpartnern für datenschutzrechtliche Belange zusammen.

7.5 Anwendungsnutzer

Die Nutzer (interne/externe Mitarbeiterinnen und Mitarbeiter, Geschäftspartner) sind bei der Erstellung, Nutzung und Verwaltung von Informationen verpflichtet, die Informationssicherheitsleitlinie und die damit verbundenen arbeitsordnenden Regelungen der Toyota Deutschland GmbH einzuhalten. Die einzelnen Nutzer sind für sämtliche Maßnahmen verantwortlich, die sie bei der Nutzung von Informationen und der damit verbundenen Systeme ergreifen.

Die Nutzer müssen verstehen, wann und warum Informationen, die zur Durchführung ihrer Geschäfte verwendet werden, zu schützen sind. Um dies zu gewährleisten, sind sie angehalten, bei Bedarf adäquate Unterstützung einzuholen. Das Unternehmen bietet entsprechende Beratung zu Informationssicherheit in der Toyota Deutschland GmbH an.

Die Nutzer, die eine Verletzung der Informationssicherheitsleitlinie und der damit verbundenen Informationssicherheitsstandards vermuten oder Kenntnis davon erlangt haben bzw. annehmen, dass Informationen nicht in geeigneter Weise geschützt sind, müssen dies unverzüglich ihrem Vorgesetzten und/oder dem Information Security Officer melden.

8 Verbesserung der Informationssicherheit

Das Informationssicherheitsmanagementsystem der Toyota Deutschland GmbH wird durch den Information Security Officer der Toyota Deutschland GmbH kontinuierlich auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeiterinnen und Mitarbeitern bekannt sind, ob sie umsetzbar, wirtschaftlich tragbar und in den Betriebsablauf integrierbar sind.

Die Geschäftsleitung unterstützt die kontinuierliche Verbesserung des Sicherheitsniveaus. Alle Mitarbeiterinnen und Mitarbeiter sind angehalten, erkannte Verbesserungspotenziale und/oder Schwachstellen an den Information Security Officer weiterzugeben. Dies kann formlos und elektronisch – per Mail an den Information Security Officer – erfolgen.

Externe Eingaben, wie von Partnern, Kunden etc., werden auf gleichem Weg kommuniziert. Hierbei kann der externe Absender den Verbesserungsprozess nicht direkt initiieren; dies erfolgt durch seinen internen Ansprechpartner der Toyota Deutschland GmbH.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung werden das angestrebte Informationssicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Informationssicherheitssituation zu verbessern und zu aktualisieren.

9 Durchsetzung der Informationssicherheitsleitlinie

Als Verstöße gegen die Informationssicherheitsleitlinie gelten vorsätzliche oder grob fahrlässige Handlungen, die

- gegen bestehende Gesetze, Verordnungen, vertragliche Verpflichtungen oder arbeitsordnende Regelungen verstoßen,
- der Toyota Deutschland GmbH an sich und/oder deren Kunden einen tatsächlichen oder potenziellen Vermögensschaden zufügen,
- den Ruf des Unternehmens, seiner Mitarbeiterinnen und Mitarbeiter oder Geschäftspartner schädigen,
- den unberechtigten Zugriff auf Daten und ggf. deren Missbrauch ermöglichen.

Verstöße gegen die Informationssicherheitsleitlinie und die entsprechenden Detailregelungen werden nicht toleriert – die Einhaltung der Sicherheitsvorgaben für die Informationsverarbeitung ist unverzichtbare Aufgabe aller Mitarbeiterinnen und Mitarbeiter und gehört zu den Leitlinien der Toyota Deutschland GmbH.

10 Erklärung der Geschäftsleitung

Die Informationssicherheitsleitlinie beinhaltet die von der Toyota Deutschland GmbH angestrebten Informationssicherheitsziele sowie die verfolgte Informationssicherheitsstrategie. Sie ist somit Anspruch und Aussage zugleich, dass ein Informationssicherheitsniveau erreicht und kontinuierlich gesteigert werden soll.

Die Informationssicherheit wird als eine Grundvoraussetzung für den Betrieb der Informations- und Kommunikationstechnik betrachtet.

Die Toyota Deutschland GmbH definiert einen umfassenden Informationssicherheitsprozess auf Basis des international anerkannten Standards ISO 27001 und setzt diesen um, mit dem Ziel eines dauerhaften und angemessenen Schutzes der Toyota Deutschland GmbH vor Risiken und Verletzungen der Informationssicherheit.

Diese Informationssicherheitsleitlinie versteht sich als einer der Grundbausteine dieses Prozesses und bildet den Rahmen für alle Aktivitäten im benannten Geltungsbereich des ISMS.

Durch diese Erklärung bekennt sich die Geschäftsleitung ausdrücklich zu den in diesem und in weiteren damit verbundenen Dokumenten enthaltenen Ansprüchen und erwartet von allen Mitarbeiterinnen und Mitarbeitern ein durchgängiges Denken und Handeln im Sinne dieser Ansprüche.

-- PROTECTED 関係者外秘
Digital unterschrieben von Andre Schmidt
Datum: 2024.11.18 10:46:12 +01'00'

André Schmidt

President Toyota Deutschland GmbH

Felix Büttner
Digital unterschrieben von Felix Büttner
Datum: 2024.11.18 14:21:20 +01'00'

Felix Büttner

Director Corporate Functions