Informationssicherheitsrichtlinie

Digital Automotive

Version: 1.1.0

Datum: 08.01.2025

Vertraulichkeit: gering

Verfügbarkeit: hoch

Integrität: hoch

Autor: Jürgen Sterr / CTO

Mitwirkende:

- Tobias Kellner / ISB

Interessierte Parteien:

- Mitarbeiter
- Kunden

Versionshistorie

Version	Datum	Geändert durch	Genehmigt von	Änderungen
1.0.0	17.07.2023	Jürgen Sterr	Erik Reiter	Dokument initial erstellt.
1.1.0	08.01.2025	Tobias Kellner	Jürgen Sterr	Formatierung & kleinere Fehler.

1 Inhalt

2 Informationssicherheitsrichtlinie

2.1 Ziele

Diese Informationssicherheitsrichtlinie der IT Manufactory GmbH legt die Vertraulichkeit, Integrität und Verfügbarkeit, sowie die Sicherstellung der Einhaltung im Unternehmen fest.

2.2 Geltungsbereich

Diese Informationssicherheitsrichtlinie gilt für die IT Manufactory GmbH und deren Mitarbeiter. Die Informationssicherheitsrichtlinie erstreckt sich auf alle Bereiche des Unternehmens.

2.3 Projektmanagement

Informationssicherheit wird im Projektmanagement unabhängig von der Art des Projekts berücksichtigt. Für Projekte, die als sicherheitskritisch eingestuft werden, ist eine Sicherheitsüberprüfung im Sinne des ISMS erforderlich. Diese Überprüfung wird vom Projektleiter, dem DevSecOps-Team und gegebenenfalls dem Informationssicherheitsbeauftragten durchgeführt und bewertet.

Es werden Grundlagen festgelegt wie:

- Verfügbarkeit von Systemen,
- Integrität, Vertraulichkeit und Verfügbarkeit,
- Zeitlicher Rahmen,
- Finanzielle Ressourcen,
- Personalaufwand,
- Projektorganisation,
- Anforderungen an Informationssicherheitsrisiken,
- Lenkungsgremium,
- Interne / externe Kunden,
- Projektleitung / Projektteam,
- Eingebundene Experten,
- Vertragswesen,
- Interessierte Parteien,
- Meilensteine,
- Ablauf- und Terminplanung,
- Risikomanagement im Projekt,
- Berichtswesen,
- Monitoring,
- Ergebnisdarstellung,
- Entscheidungen,
- Übernahme / Übergabe und
- Maßnahmenpläne.

Außerdem werden Änderungen im Projekt durch dokumentiertes Änderungsmanagement und Wiederveröffentlichungsmanagement nachvollziehbar gemacht.

2.4 Mobilgeräte und Telearbeit

Eine Richtlinie und unterstützende Sicherheitsmaßnahmen wurden implementiert, um die Risiken im Zusammenhang mit der Nutzung mobiler Geräte zu verwalten. Eine entsprechende Richtlinie wird umgesetzt und durchgesetzt.

2.5 Richtlinie zur Telearbeit

Eine Richtlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Informationen, die an Telearbeitsplätzen abgerufen, verarbeitet oder gespeichert werden, wurden implementiert. Telearbeit (Homeoffice / mobiles Arbeiten) ist grundsätzlich erlaubt. Sicherheitsmaßnahmen werden sowohl technisch als auch organisatorisch umgesetzt. Die Genehmigung erfolgt prozessgesteuert. Eine entsprechende Richtlinie wurde erstellt.

2.6 Gemeinsame Rollen und Verantwortlichkeiten in der Cloud

Unsere Informationssicherheitskontrollen basieren auf ISO/IEC 27002 für Cloud-Dienste. Die IT Manufactory GmbH stellt Cloud-Service-Kunden praktische Anleitungen und Informationen zu ihren Erwartungen an unseren Cloud-Service zur Verfügung. Die Informationssicherheitsfunktionen, Rollen und Verantwortlichkeiten für die Nutzung des Cloud-Services liegen in der Verantwortung des Kunden, da dieser die Daten eigenständig verwaltet. Die IT Manufactory GmbH und die Kunden sind sich der gemeinsamen Verantwortung in der Cloud bewusst.

2.7 Abmahnverfahren

Ein formal definiertes und bekanntgegebenes Disziplinarverfahren ist eingerichtet, um Maßnahmen gegen Mitarbeitende zu ergreifen, die einen Verstoß gegen die Informationssicherheit begangen haben. Das Disziplinarverfahren wird umgesetzt und dokumentiert.

2.8 Beendigung oder Veränderung des Arbeitsverhältnisses

Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Veränderung des Arbeitsverhältnisses weiterhin bestehen, sind definiert, dem Mitarbeitenden oder Auftragnehmer mitgeteilt und durchgesetzt. Durch das Offboarding und den Wechsel des Arbeitsverhältnisses werden die Aufgaben im Hinblick auf die Informationssicherheit bearbeitet und ihre Erfüllung wird überprüft, wenn Mitarbeitende das Unternehmen verlassen (Offboarding) oder das Arbeitsverhältnis wechseln (Wechsel des Arbeitsverhältnisses).

2.9 Wertemanagement

Werte sind die Grundlage jeder Unternehmenskultur. Die Werte in unserem Unternehmen sind:

- Inventar,
- Geschäftsprozesse,
- Immaterialgüter wie
  - Ruf des Unternhemens und
  - Sein Image,
  - Glaubwürdigkeit,
  - Zuverlässigkeit
- IT-Systeme mit:
  - Sofwate,
  - Lizenzen,
  - Hardware,
  - Netzwerkplänen,
- Gebäude & Räume sowie:
  - Einrichtungen,

- Produktinformationen wie
  - Quellcode,
  - Softwarearchitektur,
  - Dokumentation,
  - Prüflisten,
  - Schulungsunterlagen,
  - Prozessbeschreibungen,
  - Anweisungen,
  - Produktivität,
  - Kundendaten,
  - Qualitätsziele,
  - Fortschritt,
  - Sicherheit,
  - Verträge,
  - Ergebnisse,
- Datenträger,
- Dokumente,
  - Fahrzeuge,
- Mitarbeitende mit
  - Respekt,
  - Vielfalt,
  - Integrität,
  - Ehrlichkeit,
  - Offenheit,
  - Gemeinschaft,
  - Zusammenarbeit,
  - Kommunikation,
  - Kollegialität,
  - Kreativität,
  - Qualifikationen und Erfahrung,
  - Verantwortung,
  - Wertschätzung
- Rechen -und Kommunikationsdienste,
- Ausrüstung / Versorgung und
- Vermögenswerte.

Diese Werte müssen von allen Beteiligten geschützt werden. Falls sie gefährdet oder verloren gehen, muss der ISMS-Beauftragte oder das Management unverzüglich informiert werden. Diese Werte dürfen nur im festgelegten Umfang genutzt werden.

2.10 Rückgabe von Werten

2.10.1 Regulierter Ablauf für das Ausscheiden von Mitarbeitenden

Alle Mitarbeitenden und anderen Nutzer, einschließlich externer Parteien, müssen bei Beendigung des Arbeitsverhältnisses, Vertrags oder der Vereinbarung alle Vermögenswerte, die sich in ihrem Besitz befinden und dem Unternehmen gehören, zurückgeben. Beim Offboarding, also beim Verlassen des Unternehmens, wird eine Aufgabe in Form einer Checkliste zur Rückgabe der Vermögenswerte bearbeitet und überprüft.

2.10.2 Regulierter Ablauf bei der Kündigung eines Vertrags durch den Kunden

Die IT Manufactory hat eine Richtlinie zur Vertragskündigung implementiert, um sicherzustellen, dass Kunden fair und transparent behandelt werden und das Unternehmen alle relevanten gesetzlichen Anforderungen und Standards einhält. Um einen Vertrag mit einem Kunden zu kündigen, überprüfen wir zunächst den Vertrag, um sicherzustellen, dass alle Bedingungen erfüllt sind. Wenn alle Bedingungen erfüllt sind, senden wir dem Kunden eine schriftliche Kündigungsmitteilung. In dieser Mitteilung geben wir den Grund für die Kündigung sowie das Datum an, an dem die Kündigung wirksam wird.

Wir verlangen von unseren Kunden, dass sie alle von uns bereitgestellten Eigentümer und Dokumente zurückgeben, um sicherzustellen, dass unsere geistigen Eigentumsrechte geschützt bleiben. Wir überprüfen, dass wir alle von uns bereitgestellten Eigentümer zurückerhalten haben. Wir stellen sicher, dass alle ausstehenden Zahlungen oder Rückerstattungen beglichen wurden und setzen eine Frist für die Rückzahlung oder Abholung der noch bei uns befindlichen Gegenstände.

Wir dokumentieren die Beendigung des Vertrags und stellen sicher, dass wir alle relevanten Dokumente und Informationen haben, falls wir später aufgefordert werden, den Vertragsabschluss nachzuweisen. Wir sorgen dafür, dass der Kunde zufrieden ist, und gehen auf seine Bedenken ein, wenn wir den Vertrag kündigen. Wenn möglich, besprechen wir mögliche Alternativen oder Lösungen, um eine zukünftige Zusammenarbeit zu ermöglichen.

Durch die Befolgung dieses Verfahrens bei der Vertragskündigung stellen wir sicher, dass wir unseren Kunden professionell und respektvoll gegenübertreten und unsere Geschäftsbeziehungen aufrechterhalten. Wir sind stolz darauf, unseren Kunden einen hohen Qualitätsstandard zu bieten und diesen Standard auch während der Vertragskündigung aufrechtzuerhalten, sodass unsere Kunden die Gewissheit haben, dass sie stets fair und transparent behandelt werden und eine Vertragsbeendigung reibungslos und ohne unvorhergesehene Schwierigkeiten verläuft.

2.10.3 Regulierter Ablauf für die Rückgabe und sichere Entfernung von Werten

Die IT Manufactory hat ein reguliertes Verfahren für die Rückgabe und sichere Entfernung von Informationswerten implementiert, um sicherzustellen, dass Kunden fair und transparent behandelt werden und dass alle relevanten gesetzlichen Anforderungen und Standards eingehalten werden. Die Organisation nutzt ausschließlich etablierte IT-Dienste, die Richtlinien für die Rückgabe, Übertragung und/oder Löschung von Informationswerten sowie die Löschung von Informationswerten haben und jederzeit zugänglich sind. Es besteht eine vertragliche Vereinbarung zwischen der Organisation und den Cloud-Diensten, die regelmäßig überprüft wird. Darüber hinaus unterstützen wir unsere Kunden bei Anfragen zur Datenrückgabe oder Löschung von Informationswerten.

2.10.4 Ordnungsgemäße Beendigung einer Cloud-Nutzungsbeziehung

Die IT Manufactory hat eine geordnete Beendigung von Cloud-Nutzungsbeziehungen implementiert, um sicherzustellen, dass Kunden fair und transparent behandelt werden und das Unternehmen alle relevanten gesetzlichen Anforderungen und Standards einhält.

Zunächst überprüfen wir die vertragliche Kündigungsfrist, um sicherzustellen, dass alle Bedingungen erfüllt sind. Wir möchten sicherstellen, dass beide Parteien mit der Beendigung der Beziehung einverstanden sind und keine unerwarteten Probleme auftreten. Die Organisation übermittelt die Kündigungsmitteilung an den Cloud-Dienst und legt das gewünschte Kündigungsdatum fest. Der Cloud-Dienst bestätigt den Erhalt der Mitteilung, und die Organisation plant die Rückgabe der Informationswerte.

Die Organisation beginnt damit, die Informationswerte in eine sichere Umgebung zu übertragen, wie z.B. ein On-Premises-Backup oder eine andere Cloud-Plattform. Die Organisation überprüft die Vollständigkeit der Daten, testet alle erwarteten Funktionen in der neuen Umgebung und erteilt dann dem Cloud-Dienst die Erlaubnis, die Daten aus der alten Umgebung zu löschen. Der Cloud-Dienst sperrt den Zugriff auf die Dienste und löscht alle Daten, die nicht Teil der Informationswerte der Organisation sind. Der Cloud-Dienst stellt der Organisation eine abschließende Rechnung für die genutzten Dienste aus.

Der Kündigungsprozess wird abgeschlossen, und der Cloud-Dienst sowie die Organisation trennen ihre Geschäftsbeziehung.

Durch die Befolgung dieses Verfahrens stellen wir sicher, dass die Beendigung der Cloud-Nutzungsbeziehung professionell und respektvoll abgewickelt wird und dass alle relevanten Schritte ausgeführt werden, um einen reibungslosen Übergang zu gewährleisten. Die geordnete Beendigung

der Cloud-Nutzungsbeziehung durch die IT Manufactory bietet unseren Kunden die Gewissheit, dass ihre Daten und Informationen jederzeit sicher und geschützt sind und dass die Beendigung der Beziehung reibungslos und ohne unvorhergesehene Schwierigkeiten erfolgt.

2.11 Umgang mit Datenträgern

2.11.1 Umgang mit Wechseldatenträgern

Verfahren zum Umgang mit Wechseldatenträgern werden gemäß dem von der Organisation verwendeten Informationsklassifizierungsschema umgesetzt.

Der Umgang mit Wechseldatenträgern ist intern definiert:
Daten bleiben, wenn möglich, in ihrem Kontext und werden nicht auf Wechseldatenträger kopiert.

Wenn Daten auf mobile Datenträger übertragen/gespeichert werden müssen, gilt Folgendes:
Daten, die auf mobilen Datenträgern gespeichert werden (insbesondere solche, die interne, vertrauliche oder hochvertrauliche Informationen enthalten), müssen mit geeigneten Techniken (z. B. BitLocker) verschlüsselt und gesichert werden.

2.11.2 Entsorgung von Datenträgern

Datenträger, die nicht mehr benötigt werden, werden von unseren Spezialisten (SecOps-Team) unter Verwendung formaler Verfahren und Techniken sicher entsorgt.

2.11.3 Transport von Datenträgern

Datenträger, die Informationen enthalten, werden während des Transports gegen unbefugten Zugriff, Missbrauch oder Fälschung geschützt.

Der Umgang mit Datenträgern und deren Transport ist intern definiert:
Daten, die auf mobilen Datenträgern gespeichert sind und interne, vertrauliche oder streng vertrauliche Informationen enthalten können, müssen verschlüsselt und mit geeigneten Techniken (z. B. BitLocker) gesichert werden, um unbefugten Zugriff, Missbrauch oder Fälschung der Daten zu minimieren.

2.12 Zugriffssteuerungsrichtlinie

Eine Zugriffssteuerungsrichtlinie wird auf der Grundlage von Geschäfts- und Sicherheitsanforderungen erstellt, dokumentiert und regelmäßig überprüft. Die Zugriffssteuerung wird über rollenbasierte Gruppen und entsprechende Gruppenmitgliedschaften definiert. Die erforderlichen Rechte werden über die jeweiligen Rollen zugewiesen.

Es werden die folgenden Prinzipien angewendet:

- Need-to-Know-Prinzip
- So viel Zugriff wie nötig, so wenig wie möglich.

Sowohl die Policy, die Einhaltung der Zugriffssteuerung als auch die Rollen und deren Rechte werden mindestens einmal jährlich regelmäßig überprüft.

2.13 Benutzerzugriffsverwaltung

2.13.1 Registrierung / Deregistrierung

Ein formaler Prozess für die Registrierung und Abmeldung von Benutzern wurde implementiert, um die Zuweisung von Zugriffsrechten zu ermöglichen.

Wir erstellen und verwalten zwei Arten von Benutzerkonten für verschiedene Umgebungen:

- Benutzerkonten für die interne Nutzung von Anwendungen.
- Benutzerkonten für Kunden der Digital Automotive Plattform.

Für beide Arten von Benutzerkonten sind Prozesse definiert und implementiert, um die korrekte Registrierung und Abmeldung von Benutzern sicherzustellen. Zum Beispiel werden Mitarbeiterkonten während des On-Boarding-Verfahrens bei ihrem Eintritt in das Unternehmen erstellt und bei ihrem Austritt im Rahmen des Off-Boarding-Prozesses deaktiviert und gelöscht. Die Verwaltung erfolgt z. B. über Microsoft Entra ID, Azure usw.

Die IT Manufactory GmbH führt regelmäßig Prüfungen ungenutzter Zugangsdaten durch. Nach Bekanntwerden eines Sicherheitsvorfalls wird das Zurücksetzen betroffener Konten über einen organisatorischen Prozess geregelt.

Für den Cloud-Betrieb gilt zusätzlich:

Der Konfigurationsleitfaden in Atlassian Confluence ist ebenfalls der Digital Automotive Platform (Keycloak) gewidmet und behandelt das Thema der Einrichtung von Benutzern.

2.13.2 Verwaltung von privilegierten Zugriffsrechten

Die Geschäftsführung ist für diese Rollen verantwortlich. Die Zuweisung und Nutzung privilegierter Zugriffsrechte wird durch die Geschäftsführung eingeschränkt und kontrolliert. Benutzer mit speziellen administrativen oder privilegierten Rechten werden in geeigneten Rollengruppen zusammengefasst und unterliegen den entsprechenden Genehmigungen durch die Geschäftsführung. Für besonders privilegierte Rechte (z. B. Zugriff auf Firewalls, Admin-Portale usw.) muss der Benutzer ein spezielles personalisiertes Administrator-Konto verwenden; sein "normales" Benutzerkonto erhält diese Rechte nicht und kann nicht den entsprechenden Rollen zugewiesen werden.

2.13.3 Verwaltung von geheimen Authentifizierungsinformationen von Benutzern

Die Zuweisung geheimer Authentifizierungsinformationen wird bei der IT Manufactory GmbH durch einen formalen Prozess kontrolliert. Diese Informationen werden ausschließlich in verschlüsselter Form bei der IT Manufactory GmbH gespeichert. Alle Mitarbeiter verwenden ein entsprechendes Passwort-Tool. Die IT Manufactory GmbH nutzt das Passwort-Tool **Bitwarden**. Die Verpflichtung zur Nutzung des Passwort-Tools in allen Fällen ist durch entsprechende Richtlinien festgelegt.

2.13.4 Entzug oder Anpassung von Zugriffsrechten

Die Zugriffsrechte aller Mitarbeiter und externen Benutzer auf Informationen und informationstechnische Einrichtungen werden nach Beendigung des Arbeitsverhältnisses, Vertrags

oder der Vereinbarung entzogen oder im Falle einer Änderung angepasst. Die Zugriffsrechte und Rollen werden bei einer Kündigung widerrufen. Dies wird über die Personalverwaltung initiiert. Nach Beendigung einer Partnerschaft regelt der Partner-Manager die Schließung der Zugänge.

2.13.5 Beschränkung des Informationszugriffs

Der Zugang zu Informationen und Funktionen von Anwendungssystemen ist entsprechend durch Berechtigungen und eine Zugriffssteuerungspolitik eingeschränkt. Die Zugriffssteuerung wird über rollenbasierte Gruppen und die entsprechenden Gruppenmitgliedschaften definiert und eingeschränkt. Die erforderlichen Rechte werden basierend auf dem Bedarf durch die jeweiligen Rollen zugewiesen.

Es gelten die folgenden Grundsätze:

- Need-to-Know-Prinzip
- So viel Zugriff wie notwendig, so wenig wie möglich.

Sowohl die Richtlinie, die Einhaltung der Zugriffssteuerung als auch die Rollen und deren Rechte werden mindestens einmal jährlich überprüft.

Für den Cloud-Betrieb gilt zusätzlich:

Wir stellen sicher, dass bei der (Re-)Zuweisung von Speicherplatz keine Alt-Daten enthalten sind.

2.14 Kryptographie

Alle notwendigen Daten werden mittels Kryptographiedienste verschlüsselt. Alle Anwender/-innen werden in die Kryptographiedienste eingewiesen. Daten, die nicht kryptografisch verschlüsselt sind, werden dem / der ISMS-Beauftragte(n) mitgeteilt. Auf den Client-Rechnern ist ein Stammdienst installiert, der die Verschlüsselung gewährleistet. Der / die ISMS-Beauftragte prüft quartalsweise die Regelungen.

Genauere Informationen über die verwendeten kryptographischen Systeme können der entsprechenden Richtlinie entnommen werden.

2.14.1 Schlüsselverwaltung

Eine Richtlinie zur Verwendung, zum Schutz und zur Lebensdauer von kryptografischen Schlüsseln wird entwickelt und im gesamten Lebenszyklus implementiert. Richtlinien für die Verwendung, den Schutz und die Lebensdauer kryptografischer Schlüssel existieren und werden im gesamten Lebenszyklus umgesetzt.

Gültigkeitsbereiche der SSH-Schlüssel:

Der Gültigkeitsbereich definiert die Benutzer, Systeme und Anwendungen, für die der SSH-Schlüssel gilt:

- Benutzer: IT Manufactory Entwicklungsteam, DevSecOps-Team.
- Systeme: Der Zugriff auf alle Server (intern und extern) wird über SSH-Schlüssel verwaltet. DevSecOps ist verantwortlich für das Management des Zugriffs auf diese Systeme für jeden Benutzer. Benutzern wird nur dann Zugriff auf die Systeme gewährt, wenn es notwendig ist.
- Anwendungen: Entwickler müssen über ihre SSH-Schlüssel auf das GitLab der IT Manufactory zugreifen.

Inventar von Vermögenswerten:

Die Sammlung aller SSH-Schlüssel und deren Zugriffsverwendung wird in einem Git-Repository gespeichert. Damit stellen wir sicher, dass widerrufene Schlüssel und das Datum der Entfernung ebenfalls dokumentiert sind.

Richtlinie zur SSH-Schlüsselgenerierung:

Die Entwicklerkonfiguration definiert die richtige Methode zur Generierung eines SSH-Schlüsselpaares, das mit allen internen Konfigurationen kompatibel ist und gleichzeitig den Standard-Sicherheitspraktiken entspricht. Alle SSH-Schlüsselpaar werden unter Verwendung des ECDH ED25519 Kurvenalgorithmus erstellt.

Zugriffsgewährung und -entzug:

Zeitgerechter oder geplanter Zugriff auf Schlüssel wird von den DevSecOps-Teams verwaltet. Ein Benutzer kann ein Standard-Jira-Ticket erstellen, um Zugriff auf bestimmte Systeme zu erhalten. Die Anfrage des Benutzers wird dann bewertet, ihr aktiver Schlüssel wird abgerufen und der Zugriff wird dem Benutzer gewährt. Die Dauer des Zugriffs hängt von der jeweiligen Aufgabe und den Anforderungen des Benutzers ab.

2.15 Physische und Umweltbezogene Sicherheit

2.15.1 Physische Sicherheitsperimeter

Sicherheitsperimeter werden definiert und eingesetzt, um Bereiche zu schützen, in denen entweder sensible oder kritische Informationen oder informationsverarbeitende Geräte untergebracht sind.

- Der Hauptsitz in Passau ist durch ein elektronisches Zugangskontrollsystem gesichert.
- Nur autorisierte Personen haben Zugang.
- Bereiche sind durch gesperrte Zonen voneinander getrennt.
- Weitere Dokumentationen sind in der entsprechenden Richtlinie zu finden.

2.15.2 Physiche Zutrittskontrolle

Sichere Bereiche sind durch geeignete, nachverfolgbare Zugangskontrollen geschützt, um sicherzustellen, dass nur autorisierte Personen Zugang erhalten.

- Es gibt zwei Bereiche: den nicht-öffentlichen Bereich und spezielle Bereiche. Alle Zugangspunkte sind gesichert und mit AirKey-Schlössern ausgestattet.
- Die Ausgabe, Übergabe und Rückgabe von Schlüsseln wird dokumentiert.
- Die Ausgabe, Übergabe, Rückgabe und Zerstörung von AirKeys wird dokumentiert, und die Gültigkeitsdauern werden bei Bedarf festgelegt.
- Mitarbeiter werden im Rahmen ihrer Sicherheitsunterweisung auf den Umgang mit Gästen hingewiesen.
- Im Falle eines Verlusts muss der ISMS-Beauftragte sofort informiert werden.

2.15.3 Entsorgung oder Wiederverwendung von Geräten

Alle Arten von Geräten und Vorräten, die Speichermedien enthalten, werden überprüft, um sicherzustellen, dass alle sensiblen Daten und lizenzierten Softwareprodukte vor der Entsorgung oder

Wiederverwendung entfernt oder sicher überschrieben wurden. Papier, Speichermedien und andere Geräte, die Informationen enthalten, werden sicher vernichtet.

Die Entsorgung von Datenträgern geht davon aus, dass diese personenbezogene Daten enthalten. Die Experten der DevSecOps-Abteilung sammeln sie und vernichten sie sicher vor Ort. Der Zerstörungsprozess wird in der DIN 66399 beschrieben:

- Sicherheitsstufe: vertraulich (DIN 66399-1)
- Sicherheitsstufe: Festplatten und ähnliche Medien: H-4 (DIN 66399-2), Papier: P-4 (DIN 66399-2)

Dies gilt auch für Cloud-Operationen.

2.16 Unbeaufsichtigte Benutzergeräte

Benutzer stellen sicher, dass unbeaufsichtigte Geräte und Ressourcen angemessen geschützt sind. Die Richtlinie für die Aufforderung zur erneuten Authentifizierung nach Inaktivität variiert je nach Gerät:

- Für lokale PCs, Laptops, Notebooks nach 5 Minuten Inaktivität.
- Für mobile Geräte (Smartphones, Tablets, etc.) PIN (oder Passwort, mindestens 4 Zeichen) und eine Sperrzeit von 3 Minuten.
- Entnehmbare Datenträger und mobile Geräte müssen gesperrt aufbewahrt werden.

Siehe auch die Richtlinie zur Arbeitssicherheit als weiteres Dokument.

2.17Richtlinie für eine ordentliche Arbeitsumgebung und Bildschirm-Sperren

Die IT Manufactory GmbH lebt die Clean Desk Policy. Es gelten Richtlinien für eine ordentliche Arbeitsumgebung in Bezug auf Dokumente und abnehmbare Datenträger sowie für Bildschirmsperren bei der Informationsverarbeitung.

Keine Dokumente oder Datenträger, die sensible Daten enthalten, dürfen unbeaufsichtigt und unverschlossen am Arbeitsplatz liegen bleiben. Außerhalb der Arbeitszeiten müssen alle Dokumente, die sensible Daten enthalten, und mobile Geräte der Mitarbeiter sicher verwahrt werden. Zugangsdaten (wie Benutzername/Passwort) dürfen nicht schriftlich am Arbeitsplatz hinterlassen werden (z. B. am Bildschirm, unter der Tastatur oder unter dem Schreibtischpad – mit Ausnahme von zentral verwalteten Konten, die in entsprechenden Tools gemanagt werden). Vertrauliche Dokumente und Dokumente, die personenbezogene Daten enthalten, gehören NICHT in den Papierkorb, sondern müssen entweder geschreddert oder in die Papierentsorgungsbehälter abgelegt werden. Bildschirme, Postfächer und Ablagekörbe müssen so platziert werden, dass keine Besucher sie im Vorübergehen einsehen oder Dokumente unbemerkt entnehmen können. Bei kurzen Abwesenheiten muss durch Abmelden von allen Systemen oder durch Sperren des Bildschirms (mit erneuter Passwort-Eingabe) sichergestellt werden, dass niemand unbefugten Zugang zu vertraulichen Daten erhält.

Beim Verlassen eines Besprechungsraums müssen alle Arbeitsdokumente, Präsentationen, Flipcharts, abnehmbare Medien usw. mitgenommen werden. Aus hygienischen Gründen müssen außerdem alle Kaffeetassen, Becher, Gläser, leere Flaschen, Geschirr und Abfälle ordnungsgemäß entsorgt werden, und der Tisch muss sauber hinterlassen werden. Ausdrucke am Gemeinschaftsdrucker sind sofort

abzuholen. Es ist darauf zu achten, dass keine Ausdrucke oder Kopien am Drucker oder Kopierer verbleiben. Grundsätzlich wird papierlos gearbeitet, und nur in besonderen Fällen sollten Ausdrucke und Kopien angefertigt werden.

Siehe auch die Arbeitsschutzrichtlinie als weiteres Dokument.

2.18 Änderungsmanagement

Änderungen an der Organisation, den Geschäftsprozessen, der Informationsverarbeitungsausrüstung und den Systemen werden kontrolliert und in angemessener Weise kommuniziert. Alle Änderungen unterliegen dem Change-Management-Prozess, der die jeweilige Änderung steuert. Falls erforderlich, werden Schulungen durchgeführt oder Informationen erstellt.

2.19 Kapazitätskontrolle

Die Ressourcennutzung/-verwendung wird überwacht und abgeglichen, und es werden Prognosen für zukünftige Kapazitätsanforderungen erstellt, um die erforderliche Systemleistung sicherzustellen. Alle Ressourcen (IT-Infrastruktur, wie Netzwerk, Rechenleistung, Speicher) werden regelmäßig überprüft. Prognosen zur Systemauslastung und Nutzungstrends werden über geeignete Tools und Grafiken präsentiert und analysiert. Die Planung neuer Systeme, Systemerweiterungen und Leitungs-Upgrades erfolgt im Rahmen von Projekten und einem kontrollierten Change-Management, was wiederum zu entsprechenden Maßnahmen für die Kapazitätserweiterung führt. Grundsätzlich wird die Planung mit einem vorausschauenden Puffer durchgeführt, der an die Dynamik der letzten Jahre angepasst und auf die Prognosen der weiteren Entwicklungen abgestimmt ist.

2.20 Trennung von Umgebungen

Betriebsumgebungen werden strikt voneinander getrennt, um das Risiko unbefugten Zugriffs auf oder Änderungen an der Betriebsumgebung zu verringern. Zu diesem Zweck werden separate Betriebsumgebungen verwendet, und rollenbasierte Zugangsdaten werden bereitgestellt. Die Trennung gilt für die folgenden Betriebsumgebungen:

- Entwicklung,
- Test,
- Review,
- Staging,
- Demo,
- Trial,
- Produktion.

Dies wird durch geeignete Prozesse sichergestellt. Die produktiven Systeme der Kunden werden gemäß den Service Level Agreements (SLA) implementiert.

Dies betrifft insbesondere:

- Maßnahmen gegen Cyberangriffe,
- Frühzeitige Erkennung von Notfällen,
- Präventions- und Wiederherstellungsmaßnahmen sowie
- Die Sensibilisierung des Verarbeitungspersonals.

Siehe weitere Dokumentation der Datenschutzrichtlinie und SLA-Wartungsverträge.

Wo die IT Manufactory GmbH nicht für die Entwicklung verantwortlich ist (Drittanbietersysteme), dürfen keine Entwicklungssysteme vorhanden sein. Trotzdem sind auch hier Staging-/Trial-/Produktionssysteme strikt getrennt.

Für den Cloud-Betrieb gilt zusätzlich: Die IT Manufactory GmbH berücksichtigt auch die Datenschutzmaßnahmen, einschließlich Risikobewertung, für Situationen, in denen Testdaten verwendet werden sollen.

2.21 Protokollierung und Überwachung

2.21.1 Ereignissprotokollierung

Es werden Protokolle über alle Vorfälle geführt und Ereignisse überwacht. Dies umfasst:

- Ereignisprotokolle,
- Aktivitäten von Benutzern und Administratoren,
- Ausnahmen,
- Vorfälle,
- Informationssicherheitsvorfälle.

Überwachung, Alarmierung und Protokollierung erfolgen kontrolliert. Sie sind im Anwendungsmanagement verankert. Die zugehörigen Richtlinien werden von der IT Manufactory GmbH im internen Atlassian Jira Confluence Betrieb definiert.

Für den Cloud-Betrieb gilt ebenfalls:

Auf Anfrage bieten wir unseren Kunden die Möglichkeit, relevante Log-Daten zu übergeben. Die Regelmäßigkeit und Tiefe der Prüfung liegt in der Verantwortung des Kunden.

2.22 Informationsübermittlung

2.22.1Richtlinien und Verfahren für die Informationsübertragung

Formelle Richtlinien, Verfahren und Maßnahmen sind vorhanden, um den Informationsfluss für alle Arten von Kommunikationsgeräten zu schützen. Die IT Manufactory GmbH hat Regeln für den Umgang mit der Datenübertragung (Data on the Move) erlassen.

Entsprechende Verfahren und Maßnahmen wurden implementiert und werden angewendet. Dies gilt auch für den Cloud-Betrieb.

2.22.2 Vereinbarungen über den Informationsaustausch

Vereinbarungen regeln den sicheren Transfer von Unternehmensinformationen zwischen der Organisation und externen Parteien. Die Handhabung des Datentransfers (Daten in Bewegung) wird mit externen Partnern vereinbart.

Diese Vereinbarungen sind in den entsprechenden Verträgen zu finden:

- unter anderem in Geheimhaltungsvereinbarungen (NDA),
- Lizenzvereinbarungen für Systemzugang (DA),

- den entsprechenden Leistungsbeschreibungen (die Teil des Vertrags sind) oder individuellen Service-Level-Vereinbarungen (SLA) mit Kunden.

2.22.3 Elektronische Nachrichten

Informationen in elektronischen Nachrichten sind angemessen geschützt. Alle übertragenen Daten (Daten in Bewegung) werden spätestens bei einem Zonentausch verschlüsselt. Die Verschlüsselung erfolgt mindestens mit TLS 1.2 (mit AES 256 Bit).

2.22.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen, die den Bedarf der Organisation zum Schutz von Informationen widerspiegeln, werden identifiziert, regelmäßig überprüft und dokumentiert. Vertraulichkeitsvereinbarungen bestehen sowohl für den internen als auch externen Gebrauch. Verantwortliche Stellen (aus den Bereichen Recht, Datenschutz und Personalwesen) sind für den Inhalt zuständig und pflegen diesen regelmäßig. Quellen für Änderungen können Audits, Gesetzgebungen, Anforderungen im Austausch mit Geschäftspartnern (Lieferanten, Kunden) und Änderungen im Bestand schutzbedürftiger Vermögenswerte sein.

Inhalte von Geheimhaltungsvereinbarungen (NDA), auch wenn sie von der anderen Partei erstellt werden:

- beteiligte Personen/Organisationen,
- die Art der im Vertrag abgedeckten Informationen,
- das Thema des Vertrages,
- die Gültigkeitsdauer des Vertrages,
- die Verantwortlichkeiten der Verpflichteten.

Geheimhaltungsvereinbarungen enthalten Bestimmungen für den Umgang mit schutzbedürftigen Informationen über die vertragliche Beziehung hinaus. Ein Prozess, der die Gültigkeitsdauer vorübergehender Geheimhaltungsvereinbarungen überwacht und die rechtzeitige Verlängerung von Geheimhaltungsvereinbarungen initiiert, wurde definiert und umgesetzt.

Für den Cloud-Betrieb gilt zusätzlich:

- Kunden und Partner unterschreiben zu Beginn des Vertrages Standardverträge mit entsprechender Geheimhaltungspflicht, auch in der Datenverarbeitung.
- Mitarbeiter der IT Manufactory GmbH sind im Rahmen ihres Arbeitsvertrages zur Geheimhaltung verpflichtet und werden regelmäßig diesbezüglich geschult.
- Diese Verträge enthalten eine Zweckbindung gemäß der Verpflichtung zur Weisungsbefolgung im Rahmen der gegenwärtigen Auftragsverarbeitung.
- Die Geheimhaltungspflicht erstreckt sich über die Dauer des Vertrages hinaus.

2.23 Sicherheit in Entwicklungs- und Supportprozessen über die Grundlagen hinaus

2.23.1 Richtlinie für sichere Entwicklung

Regeln für die Entwicklung von Software und Systemen sind definiert und auf Entwicklungen innerhalb der Organisation angewendet. Im Rahmen des SCRUM-Prozesses wird die Berücksichtigung

von Sicherheitsinteressen bei der Entwicklung und Wartung von Software und Systemen geregelt und in Form von Prozessen und HowTos definiert. Für spezifische Prozesse in der Softwareentwicklung werden Themenverantwortliche benannt. Weitere Informationen finden sich im Agile Manifesto und der entsprechenden Richtlinie.

2.23.2 Verfahren zur Verwaltung von Systemänderungen

Die Implementierung von Änderungen muss einem formalen Änderungssteuerungsverfahren unterliegen. Die Umsetzung von Änderungen erfolgt im Rahmen eines Change-Management-Prozesses durch Fachexperten, die die Release-Planung und Kommunikation mit dem Kunden koordinieren und Softwareänderungen mit spürbaren Auswirkungen für die Kunden bewerten.

2.23.3 Einschränkung von Änderungen an Softwarepaketen

Änderungen an Softwarepaketen werden nicht gefördert, sind auf das notwendige Minimum beschränkt und unterliegen einer strengen Steuerung. Im Rahmen des SCRUM-Prozesses wird in Form von HowTos geregelt, wie Softwareänderungen vor der Freigabe bewertet werden sollen. Die Änderungen werden von den Produktmanagern, die für das jeweilige Thema verantwortlich sind, gesteuert. Bei maßgeschneiderten Systemen werden Änderungen auf Anfrage des Kunden vorgenommen.

2.23.4 Grundsätze für die Analyse, Entwicklung und Wartung von Systemen

Grundsätze für die Analyse, Entwicklung und Wartung sicherer Systeme sind definiert, dokumentiert, auf dem neuesten Stand gehalten und auf jedes Implementierungsprojekt eines Informationssystems angewendet. Regeln, die sicherstellen, dass die Grundsätze für die Analyse, Entwicklung und Wartung sicherer Systeme in die entsprechenden Prozesse, die dazugehörigen Anweisungen (HowTos) sowie durch die Vorgaben des Sicherheitsleitfadens und die Bereitstellung des Rahmens integriert werden, sind festgelegt.

2.23.5 Sichere Entwicklungsumgebung

Organisationen schaffen sichere Entwicklungsumgebungen für Systementwicklungs- und Systemintegrationsprojekte über den gesamten Entwicklungszyklus hinweg und schützen diese angemessen. Die Bereitstellung, der Betrieb und die Wartung einer sicheren Entwicklungsumgebung werden durch entsprechende Fachverantwortliche sichergestellt. Die Sicherheit und Aktualität der Entwicklungsumgebung sowie der gesamten Anwendungslandschaft werden regelmäßig im Rahmen des Anwendungsmanagements überprüft.

2.23.6 Ausgelagerte Entwicklung

Die Organisation überwacht und kontrolliert die Aktivitäten der ausgelagerten Systementwicklung. Im Rahmen des Qualitätsmanagements wird geregelt und in Form von Prozessen und HowTos definiert, wie Aktivitäten im Zusammenhang mit der ausgelagerten Systementwicklung integriert und überwacht oder vorangetrieben werden. Die Hauptverantwortung hierfür liegt beim jeweiligen Partner-Manager des jeweiligen Entwicklungspartners.

2.23.7 Testen der Systemsicherheit

Die Sicherheitsfunktionen werden während der Entwicklung getestet. Im Rahmen der Qualitätssicherung werden neue Entwicklungen manuell auf die definierten Anforderungen sowie auf Datenschutz- und Sicherheitsanforderungen vor der Freigabe getestet. Dafür gibt es Testmanager, die das Testmanagement übernehmen. Darüber hinaus sorgen automatische Tests kontinuierlich für den Schutz vor unbeabsichtigten Nebenwirkungen der Entwicklung.

2.23.8 Systemabnahmeprüfung

Abnahmetestprogramme und zugehörige Kriterien werden für neue Informationssysteme, Updates und neue Versionen definiert. Im Rahmen des Qualitäts-, Änderungs- und Release-Managements werden Prozesse und HowTos festgelegt, die vorschreiben, dass vor der Freigabe neuer Informationssysteme, Updates oder neuer Versionen entsprechende Abnahmetests durchgeführt, geplant und von den verantwortlichen Personen gesteuert werden. Regelmäßige Wartungsarbeiten (Softwarewartung) werden rechtzeitig geplant und zusammen mit unregelmäßiger Wartung dokumentiert.

2.24 Umgang mit Informationssicherheitsvorfällen und Verbesserungen

2.24.1 Verantwortlichkeiten und Verfahren

Verantwortlichkeiten und Verfahren für die Handhabung von Informationssicherheitsvorfällen sind festgelegt, um eine schnelle, effektive und ordnungsgemäße Reaktion sicherzustellen. Der Prozess zur Meldung von Sicherheitsvorfällen ist organisiert und wird regelmäßig kommuniziert. Zu diesem Zweck bietet die Meldung mehrere Optionen zur Auslösung und wird mit Unterstützung von Werkzeugen bearbeitet. Mögliche Empfänger (z.B. für IT-Sicherheitsvorfälle, Datenschutzverletzungen, Notfälle) sind durch Rollen verankert und geschult.

Für den Cloud-Betrieb gilt zusätzlich:

Die IT Manufactory GmbH hat einen internen Prozess zur Meldung und Handhabung von Sicherheitsvorfällen eingerichtet. Unter anderem wird die Kritikalität nach Sicherheitskriterien analysiert und im weiteren Verfahren berücksichtigt. Falls erforderlich, sieht der Prozess eine Zusammenarbeit mit den betroffenen Kunden vor, wie vereinbart.

2.24.2 Meldung von Informationssicherheitsereignissen

Informationssicherheitsereignisse werden so schnell wie möglich dem Informationssicherheitsbeauftragten und dem Datenschutzbeauftragten gemeldet. Die IT Manufactory GmbH hat Prozesse für Sicherheitsvorfälle implementiert, um sicherzustellen, dass Informationssicherheitsereignisse schnellstmöglich über die entsprechenden, bekannten Kanäle gemeldet und bearbeitet werden. Dies umfasst Prozesse sowohl für den regulären Betrieb (Sicherheitsvorfall- und Incident-Management) als auch für außergewöhnliche Situationen (Prozesse im Notfallmanagement sowie Verfügbarkeitsmanagement oder Datenschutzverletzungen im Bereich Datenschutz). Kunden können sich bei allen Sicherheitsanliegen und -meldungen an das Service

Management der IT Manufactory GmbH über die ihnen zur Verfügung stehenden Kanäle wenden. Von hier aus werden erste Reaktionen sowie Eskalationen gesteuert. Im Falle eigener Sicherheitsvorfälle kontaktiert die IT Manufactory GmbH sofort die betroffenen Kunden.

2.24.3 Bewertung und Entscheidung über Informationssicherheitsereignisse

Informationssicherheitsereignisse werden bewertet, und es wird entschieden, ob sie als Informationssicherheitsvorfälle klassifiziert werden sollten.

Elementare Sicherheitsvorfälle, Ereignisse und Bedrohungen:

- Ausfall oder Fehlfunktion des Kommunikationsnetzwerks
- Fehlfunktion oder Ausfall von Dienstleistern
- Falschplanung oder fehlende Anpassung
- Offenlegung sensibler Informationen
- Informationen oder Produkte aus unsicheren Quellen
- Manipulation von Hardware oder Software
- Manipulation von Informationen
- Unerlaubtes Eindringen in IT-Systeme
- Fehlfunktion von Geräten oder Systemen
- Störung von Geräten oder Systemen
- Mangel an Ressourcen
- Software-Schwachstellen oder Fehler
- Verstöße gegen Gesetze oder Vorschriften
- Unerlaubte Nutzung oder Verwaltung von Geräten und Systemen
- Falsche Nutzung oder Verwaltung von Geräten und Systemen
- Fehlgebrauch von Berechtigungen
- Personalversagen
- Verweigerung von Aktionen
- Missbrauch personenbezogener Daten
- Schadhafter Code (Malware)
- Verhinderung von Diensten (Denial of Service)
- Sabotage
- Verlust der Integrität schutzbedürftiger Informationen

2.24.4 Reaktion auf Informationssicherheitsvorfälle

Informationssicherheitsvorfälle werden gemäß dokumentierten Verfahren bearbeitet. Die IT Manufactory GmbH hat Prozesse für Sicherheitsvorfälle implementiert, um sicherzustellen, dass Informationssicherheitsereignisse so schnell wie möglich über die entsprechenden, bekannten Kanäle gemeldet und bearbeitet werden. Dies umfasst Prozesse für den regulären Betrieb (Sicherheitsvorfall- und Incident-Management) sowie für außergewöhnliche Situationen (Prozesse im Notfallmanagement, im Verfügbarkeitsmanagement oder bei Datenschutzverletzungen im Bereich Datenschutz).

2.24.5 Erkenntnisse aus Informationssicherheitsvorfällen

Erkenntnisse, die aus der Analyse und Lösung von Informationssicherheitsvorfällen gewonnen werden, werden genutzt, um die Wahrscheinlichkeit des Auftretens oder die Auswirkungen

zukünftiger Vorfälle zu verringern. Die IT Manufactory GmbH hat einen Prozess für Sicherheitsvorfälle sowie einen Incident-Management-Prozess etabliert. Dies umfasst auch die Bearbeitung der Ergebnisse aus Sicherheitsvorfällen und deren langfristige Behandlung. Dasselbe gilt für das Notfallmanagement, das Verfügbarkeitsmanagement oder die Bearbeitung von Datenpannen. Regelmäßige Meetings stellen sicher, dass die Erkenntnisse ausgewertet und bearbeitet werden. Diese dienen auch als Input für das ISMS (zum Beispiel in Bezug auf die Korrektur der Eintrittswahrscheinlichkeiten, Risikobewertung und Risikobehandlung).

2.25 Sammlung von Beweismitteln

Die Organisation bestimmt und wendet die Identifizierung, Sammlung, Aufzeichnung und Aufbewahrung von Informationen an, die als Beweismittel dienen können. Die Beweismittel werden vom ISMS-Beauftragten bzw. den ISMS-Beauftragten gesammelt und verarbeitet. Die Geschäftsführung entscheidet, ob eine strafrechtliche Untersuchung eingeleitet wird.

Beweismittel:

- Systemprotokolle
- Logdateien
- Notizen
- Fotos von Bildschirminhalten
- Datenmedien
- Digitale Informationen
- Personen
- Aktivitäten
- Fakten

2.26 Compliance

2.26.1 Einhaltung rechtlicher und vertraglicher Anforderungen

Das Risiko der Nichteinhaltung rechtlicher, regulatorischer, selbst auferlegter oder vertraglicher Verpflichtungen in Bezug auf die Informationssicherheit wird berücksichtigt.

2.26.2 Datenschutz und Schutz personenbezogener Informationen

Datenschutz und Schutz personenbezogener Informationen werden, sofern zutreffend, in Übereinstimmung mit den Anforderungen der relevanten Gesetze und Vorschriften gewährleistet. Ein Datenschutzbeauftragter wurde ernannt, um die Einhaltung der relevanten Datenschutzgesetze sicherzustellen. Schulungs- und Weiterbildungsmaßnahmen zu diesen Themen sowie zur Sensibilisierung wurden für Mitarbeiter eingerichtet. Für externe Mitarbeiter kann über unser Trust Center Kontakt aufgenommen werden.

2.26.3 Überprüfungen der Informationssicherheit

Die Informationssicherheit wird regelmäßig im gesamten Unternehmen auditiert. Alle Abteilungen überprüfen zusätzlich die Informationssicherheit in ihren eigenen Bereichen. Die Ergebnisse werden in die Bewertung der Informationssicherheit einbezogen.

2.26.4 Unabhängige Überprüfung der Informationssicherheit

Der Ansatz der Organisation zur Verwaltung der Informationssicherheit und deren Umsetzung wird in regelmäßigen Abständen oder bei wesentlichen Änderungen unabhängig überprüft.

Wir unterziehen uns regelmäßigen externen Zertifizierungs-Audits gemäß:

- Unabhängiger Audit durch die Zertifizierer QM ISO 9001,
- Unabhängiger Audit durch die Zertifizierer ISMS ISO 27001,
- Unabhängiger Audit durch die Zertifizierer TISAX.

Überprüft werden:

- Zielvorgaben der Maßnahmen,
- Maßnahmen,
- Richtlinien,
- Prozesse,
- Verfahren.

Die Ergebnisse werden in einem Auditbericht zusammengefasst. Derzeit halten wir ein jährliches Audit für ausreichend. Zusätzlich werden speziell angesetzte Audits durch die ISMS-Beauftragten mit den Abteilungen bei Ereignissen und Vorfällen im Zusammenhang mit der Informationssicherheit durchgeführt.

Weitere Audits werden von Dritten durchgeführt, zum Beispiel zur Überprüfung der Datensicherheit:

- Überprüfung durch Kunden im Rahmen der Softwareintegration und -implementierung,
- Überprüfung durch Kunden im Rahmen von Sicherheits-Selbstbewertungsfragen.

In einigen Fällen können auch die Audits der technischen und organisatorischen Maßnahmen (TOMs) gemäß Artikel 28 der DSGVO durch unsere Geschäftspartner im Rahmen von Audits für die Auftragsverarbeitung bewertet werden.

Für den Cloud-Betrieb gilt zusätzlich:

- Die IT Manufactory GmbH bietet ihren Kunden eine breite Palette an Informationen, um sich von einem ordnungsgemäßen Betrieb zu überzeugen.
- Die IT Manufactory GmbH lässt sich von unabhängigen, akkreditierten Stellen auditieren und stellt geeignete Nachweise wie Zertifikate zur Verfügung.

2.26.5 Einhaltung von Sicherheitsrichtlinien und -standards

Die leitenden Führungskräfte überprüfen regelmäßig die Einhaltung der geltenden Sicherheitsrichtlinien, -standards und aller anderen Sicherheitsanforderungen für die Informationsverarbeitung und -verfahren innerhalb ihrer Zuständigkeitsbereiche.

Wir haben ein mehrstufiges Konzept für diese Aufgabe:

- Ständige Verantwortung und Prüfung durch die Rolle des Sicherheitsbeauftragten.
- Regelmäßige Meetings zu Informationssicherheit und technischer Verschuldung.
- Regelmäßige interne Audits; mit Kreuzprüfung relevanter Sicherheitsrichtlinien und Stichprobenprüfung.

- Regelmäßige Erinnerungsschulungen und Auffrischungstrainings.
- Projektgetriebene Sicherstellung, dass notwendige Aktivitäten durchgeführt werden.
- Strategische Meetings wie z.B. Roadmap-Planung.

2.26.6 Überprüfung der technischen Einhaltung

Informationssysteme werden regelmäßig auf die Einhaltung der Informationssicherheitsrichtlinien und -standards der Organisation überprüft.

Dafür haben wir mehrere Situationen:

- Regelmäßige Prüfungen im Rahmen des Änderungsmanagements durch die IT-Betriebsabteilung.
- Ständige Verantwortung und Prüfung durch die Verantwortlichen für die Richtlinien sowie die Rolle des Sicherheitsbeauftragten.
- Regelmäßige Überprüfungen aus datenschutzrechtlicher Perspektive durch den Datenschutzbeauftragten.
- Regelmäßige interne und externe Audits für ISO 9001, ISO 27001, TISAX.
- Regelmäßige Termine im Meeting zu Informationssicherheit und technischer Verschuldung.
- Regelmäßige Kontrolle und Wartung der Kontrollen.

IT Manufactory GmbH
Brunngasse 4, 94032 Passau / Deutschland
Tel: +49 (0) 800 14 14 14 7
E-Mail: info@digital-automotive-supplier.com
Web: https://digital-automotive-supplier.com