5.1.1 Information Security Policy

Informationssicherheit im Projektmanagement

Informationssicherheit wird im Projektmanagement berücksichtigt, ungeachtet der Art des Projekts. Bei als sicherheitskritisch eingestuften Projekten ist ein Sicherheits-Check im Sinne des ISMS erforderlich.
Dieser Check wird vom Projektleiter, dem DevSecOps und ggfs. dem Sicherheitsbeauftragten durchgeführt und bewertet.

Dabei richtet sich der Blick u. a. auf:

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

Des Weiteren werden im Projekt Änderungen durch dokumentiertes Change-Management & Release-Management nachvollziehbar gemacht.

Richtlinie zu Mobilgeräten

Eine Richtlinie und unterstützende Sicherheitsmaßnahmen sind umgesetzt, um die Risiken, welche durch die Nutzung von Mobilgeräten bedingt sind, zu handhaben.
Eine entsprechende Richtlinie ist implementiert und wird durchgesetzt.

Richtlinie zur Telearbeit

Eine Richtlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Information, auf die von Telearbeitsplätzen aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden, sind umgesetzt.
Telearbeit (Home Office / Mobiles arbeiten) ist grundsätzlich zugelassen. Sicherheitsmaßnahmen finden sowohl technisch als auch organisatorisch statt. Eine Freigabe erfolgt prozessgesteuert. Eine entsprechende Richtlinie ist etabliert.

Gemeinsame Rollen und Verantwortlichkeiten innerhalb einer Cloud-Computing-Umgebung

Informationssicherheitskontrollen basierend auf ISO/IEC 27002 für Cloud-Dienste:
IT Manufactory GmbH stellt Cloud Service-Kunden praktische Anleitungen und Informationen im Hinblick auf ihre Erwartungen an unseren Cloud Service zur Verfügung.
Informationssicherheitsfunktionen, -rollen und -verantwortlichkeiten für die Nutzung seines Cloud Service obliegt dem Kunden, da nur er die Daten selbst verwaltet.
IT Manufactory GmbH und Kunden sind sich der gemeinsamen Verantwortung in der Cloud bewusst.

Maßregelungsprozess

Ein formal festgelegter und bekanntgegebener Maßregelungsprozess ist eingerichtet, um Maßnahmen gegen Beschäftigte zu ergreifen, die einen Informationssicherheitsverstoß begangen haben.
Der Maßregelungsprozess ist implementiert und dokumentiert.

Beendigung oder Änderung der Beschäftigung

Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, sind festgelegt, dem Beschäftigten oder Auftragnehmer mitgeteilt und durchgesetzt.
Durch das Off Boarding und Change of Employment werden beim Austritt (Off Boarding) von Mitarbeitern oder Änderung der Beschäftigung (Change of Employment) die zu erledigenden Aufgaben bezüglich der Informationssicherheit bearbeitet und deren Erfüllung überprüft.

Verwaltung der Werte

Werte sind das Fundament für die IT Manufactory Unternehmenskultur.

<u>Werte in unserem Unternehmen sind:</u>

- Inventar,
- Geschäftsprozesse,
- Immaterielle Werte wie:
  - Ruf des Unternehmens und
  - sein Image,
  - Glaubwürdigkeit,
  - Verlässlichkeit,
- Produkt Informationen wie:
  - Quellcode,
  - Softwarearchitektur,
  - Dokumentation,
  - Protokolle,
  - Checklisten,
  - Schulungsunterlagen,
  - Prozessbeschreibungen,
  - Anweisungen,
  - Produktivität,
  - Kundendaten,
  - Qualitätsziele,
  - Fortschritte,
  - Sicherheit,
  - Verträge,
  - Ergebnisse,
- Datenträger,
- Dokumente,
- IT-Systeme mit:
  - Software,
  - Lizenzen,
  - Hardware,
  - Netzplan,
- Gebäude & Räume sowie Einrichtungen,
- Fahrzeuge,
- Mitarbeiter/-innen mit:
  - Respekt,
  - Vielfalt,
  - Integrität,
  - Aufrichtigkeit,
  - Offenheit,
  - Gemeinschaft,
  - Teamarbeit,
  - Kommunikation,
  - Kollegialität,
  - Kreativität,
  - Qualifikationen und
  - Erfahrungen,
  - Verantwortung,
  - Wertschätzung,
- Rechen und Kommunikationsdienste,
- Betriebsmittel und Versorgungseinrichtungen,
- Vermögenswerte.

Diese Werte sind von allen Beteiligten zu schützen. Falls sie beeinträchtigt oder verloren gehen können, muss sofort der / die ISMS-Beauftragte(r) oder die Geschäftsführung informiert werden.
Diese Werte dürfen im festgelegten Umfang verwendet werden.

Rückgabe von Werten

Geregelte Verfahrensweise beim Weggang von Mitarbeitern:
Alle Beschäftigten und sonstige Benutzer, die zu externen Parteien gehören, geben bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung sämtliche in ihrem Besitz befindlichen Werte,
die der Organisation gehören, zurück. Im Off Boarding wird bei Austritt eine Aufgabe, in Form einer Checkliste, zur Rückgabe von Werten bearbeitet und überprüft.

Geregelte Verfahrensweise bei Vertragsbeendigung eines Kunden:
Die IT Manufactory hat eine geregelte Verfahrensweise bei Vertragsbeendigung implementiert, um sicherzustellen, dass Kunden fair und transparent behandelt werden und das Unternehmen dabei alle relevanten rechtlichen Bestimmungen und Normen einhält.

Um einen Vertrag mit einem Kunden zu beenden, prüfen wir zunächst den Vertrag, um sicherzustellen, dass alle Bedingungen erfüllt wurden. Wenn alle Bedingungen erfüllt wurden, senden wir dem Kunden eine schriftliche Benachrichtigung über die Beendigung des Vertrags. In dieser Benachrichtigung geben wir den Grund für die Beendigung und das Datum, an dem die Beendigung wirksam wird, an.

Wir fordern den Kunden auf, alle von uns zur Verfügung gestellten Eigentum und Dokumente zurückzugeben, um sicherzustellen, dass alle unsere geistigen Eigentumsrechte geschützt bleiben. Wir überprüfen, ob wir alle von uns zur Verfügung gestellten Gegenstände zurückerhalten haben. Stellen wir sicher, dass alle fälligen Zahlungen oder Rückerstattungen ausgeglichen wurden und legen wir eine Frist für die Rückzahlung oder Abholung von Gegenständen fest, die noch bei uns sind.

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

Durch die Einhaltung dieser Verfahrensweise bei Vertragsbeendigungen können wir sicherstellen, dass wir professionell und respektvoll mit unseren Kunden umgehen und unsere Geschäftsbeziehungen aufrechterhalten. Wir sind stolz darauf, unseren Kunden einen hohen Qualitätsstandard zu bieten und diesen auch bei Vertragsbeendigungen beizubehalten und gibt unseren Kunden die Sicherheit, dass sie jederzeit fair und transparent behandelt werden und dass eine Vertragsbeendigung reibungslos und ohne unvorhergesehene Schwierigkeiten abläuft.

Geregelte Verfahrensweise bei Rückgabe und sicheres Entfernen von Informationswerten bei Cloud-Diensten:
Die IT Manufactory hat eine geregelte Verfahrensweise für die Rückgabe und sicheres Entfernen von Informationswerten implementiert, um sicherzustellen, dass Kunden fair und transparent behandelt werden und das Unternehmen dabei alle relevanten rechtlichen Bestimmungen und Normen einhält.

Die Organisation verwendet ausschließlich etablierte IT-Services und IT-Dienste welche Richtlinien zur Rückgabe, Übertragung und/oder Löschung von Informationswerten verfügen und zu jederzeit abrufbar sind.

Eine vertragliche Regelung zwischen der Organisation und den Cloud-Diensten besteht und wird regelmäßig überprüft.
Wir unterstützt unsere Kunden auch bei Anfragen zu Daten-Rückgabe bzw.
Löschung von Informationswerten.

Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses:
Die IT Manufactory hat eine geordnete Beendigung von Cloud-Nutzungs-Verhältnissen implementiert, um sicherzustellen, dass Kunden fair und transparent behandelt werden und das Unternehmen dabei alle relevanten rechtlichen Bestimmungen und Normen einhält.


Zunächst prüfen wir die vertragliche Kündigungsfrist, um sicherzustellen, dass alle Bedingungen erfüllt wurden.
Wir möchten sicherstellen, dass beide Parteien mit der Beendigung des Verhältnisses einverstanden sind und dass keine unerwarteten Probleme auftreten.


Die Organisation übermittelt dem Cloud-Dienst die Kündigung und bestimmt das gewünschte Kündigungsdatum.


Der Cloud-Dienst bestätigt den Erhalt der Kündigung und die Organisation plant die Rückführung der Informationswerte.


Die Organisation beginnt mit der Rückführung der Informationswerte in eine sichere Umgebung, wie z.B. ein lokales Backup oder eine andere Cloud-Plattform.


Die Organisation überprüft die Vollständigkeit der Daten, testet alle erwarteten Funktionen in der neuen Umgebung und erteilt dem Cloud-Dienst im Anschluss die Freigabe zur Löschung der Daten aus der alten Umgebung.


Der Cloud-Dienst deaktiviert den Zugriff auf die Dienste und löscht alle Daten, die nicht Teil der Informationswerte der Organisation sind.


Der Cloud-Dienst stellt der Organisation eine Endabrechnung für die genutzten Dienste.


Der Terminierungsprozess ist abgeschlossen, der Cloud-Dienst und die Organisation trennen ihre Geschäftsbeziehungen.

Indem wir diese Verfahrensweise befolgen, können wir sicherstellen, dass die Beendigung des Cloud-Nutzungs-Verhältnisses in einer professionellen und respektvollen Weise abläuft und dass alle relevanten Schritte ausgeführt wurden, um einen reibungslosen Übergang zu gewährleisten. Die geordnete Beendigung von Cloud-Nutzungs-Verhältnissen der IT Manufactory gibt unseren Kunden die Sicherheit, dass ihre Daten und Informationen jederzeit sicher und geschützt sind und dass die Beendigung des Verhältnisses reibungslos und ohne unvorhergesehene Schwierigkeiten abläuft.

Ordnungsgemäße Beendigung einer Cloud-Nutzungsbeziehung
IT Manufactory hat ein geordnetes Verfahren zur Beendigung von Cloud-Nutzungsverhältnissen eingeführt, um sicherzustellen, dass die Kunden fair und transparent behandelt werden und das Unternehmen alle relevanten rechtlichen Anforderungen und Standards einhält.

Zunächst überprüfen wir die vertragliche Kündigungsfrist, um sicherzustellen, dass alle Bedingungen erfüllt sind.

Wir wollen sicherstellen, dass beide Parteien mit der Beendigung der Geschäftsbeziehung einverstanden sind und dass keine unerwarteten Probleme auftreten.

Das Unternehmen übermittelt die Kündigung an den Cloud-Dienst und legt den gewünschten Kündigungstermin fest.

Der Cloud-Service bestätigt den Erhalt der Kündigung, und das Unternehmen plant die Rückgabe der Datenbestände.

Die Organisation beginnt mit der Rückführung der Informationsbestände in eine sichere Umgebung, z. B. ein Backup vor Ort oder eine andere Cloud-Plattform.

Die Organisation prüft die Vollständigkeit der Daten, testet alle erwarteten Funktionen in der neuen Umgebung und gibt dem Cloud-Service dann grünes Licht für die Löschung der Daten aus der alten Umgebung.

Der Cloud-Dienst deaktiviert den Zugang zu den Diensten und löscht alle Daten, die nicht zu den Informationsbeständen der Organisation gehören.

Der Cloud-Dienst stellt der Organisation eine Endabrechnung für die in Anspruch genommenen Dienste aus.

Der Kündigungsprozess ist abgeschlossen, und der Cloud-Dienst und die Organisation beenden ihre Geschäftsbeziehung.

Durch dieses Verfahren können wir sicherstellen, dass die Beendigung der Cloud-Nutzungsbeziehung professionell und respektvoll gehandhabt wird und dass alle relevanten Schritte für einen reibungslosen Übergang durchgeführt wurden. Die geordnete Beendigung des Cloud-Nutzungsverhältnisses durch die IT-Manufaktur gibt unseren Kunden die Gewissheit, dass ihre Daten und Informationen jederzeit sicher sind und dass die Beendigung des Verhältnisses reibungslos und ohne unvorhergesehene Schwierigkeiten verläuft.

Handhabung von Datenträgern

Handhabung von Wechseldatenträgern

Verfahren für die Handhabung von Wechseldatenträgern sind entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema umgesetzt.

Der Umgang mit Wechselmedien ist internen festgelegt:

Daten bleiben wann immer möglich in ihrem Kontext und werden nicht auf mobile Datenträger kopiert.

Sollten doch Daten auf mobile Datenträger verbracht/gespeichert werden müssen, dann gilt:

Daten, die auf mobile Datenträger abgelegt werden (insbesondere, die interne, vertrauliche oder streng vertrauliche Informationen beinhalten), müssen durch entsprechende Techniken (z. B. Bitlocker) verschlüsselt und gesichert werden.

Entsorgung von Datenträgern

Nicht mehr benötigte Datenträger werden sicher und unter Anwendung formaler Verfahren und Techniken von unseren Spezialisten (SecOps Team) entsorgt.

Transport von Datenträgern

Datenträger, die Information enthalten, sind während des Transports vor unbefugtem Zugriff, Missbrauch oder Verfälschung geschützt.

Der Umgang mit Datenträgern und ihrem Transport ist internen festgelegt:

Daten, die auf mobile Datenträger abgelegt werden und interne, vertrauliche oder streng vertrauliche Informationen beinhalten können, müssen durch entsprechende Techniken (z. B. Bitlocker) verschlüsselt und gesichert werden num unerlaubten Zugriff, Missbrauch oder Verfälschung der Daten zu minimieren.

Zugangssteuerungsrichtlinie

Eine Zugangssteuerungsrichtlinie ist auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen erstellt, dokumentiert und überprüft.

Die Zugangssteuerung wird über rollenbasierte Gruppen und entsprechende Gruppenzugehörigkeiten festgelegt. Die benötigten Rechte werden über die jeweiligen Rollen zugeteilt.

Grundlegend gilt:

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

Sowohl die Richtlinie, das Einhalten der Zugangssteuerung, als auch die Rollen und deren Rechte werden regelmäßig mindestens einmal pro Jahr überprüft.

Benutzerzugangssverwaltung

Registrierung und Deregistrierung von Benutzern

Ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern ist umgesetzt, um die Zuordnung von Zugangsrechten zu ermöglichen.

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

- Benutzerkonten für die Intern Verwendung von Anwendungen.
- Benutzerkonten für Kunden der Digital Automotive Platform.

Für beide Benutzerkontenarten sind Prozesse definiert und umgesetzt, die das korrekte Registrieren und Deregistrieren von Benutzern sicherstellen.

Z.B. werden Mitarbeiterkonten durch Eintritt ins Unternehmen durch das On Boarding angelegt und durch Ausscheiden Off Boarding deaktiviert und gelöscht.

Die Verwaltung erfolgt z.B. über Microsoft Active Directory, Azur, etc.

IT Manufactory GmbH führt in regelmäßigen Abständen Überprüfungen auf ungenutzte Zugangsdaten durch.

Nach Bekanntwerden einer Kompromittierung wird das Zurücksetzen betroffener Accounts über einen organisatorischen Prozess geregelt.

Für den Cloud-Betrieb gilt zusätzlich:

Der Konfigurationsleitfaden in Atlassian Confluence widmet sich auch der Digital Automotive Platform (Key Cloak) zum Thema Einrichtung von Usern.

Verwaltung privilegierter Zugangsrechte

Verantwortliche für diese Rollen ist die Geschäftsleitung.

Zuteilung und Gebrauch von privilegierten Zugangsrechten ist eingeschränkt und wird von der Geschäftsleitung gesteuert.

Anwender mit besonderen administrativen oder privilegierten Rechten sind in geeigneten Rollengruppen zusammengefasst und unterliegen den entsprechenden Freigaben durch die Geschäftsleitung.

Für besonders privilegierte Rechte (z. B. Firewall-Zugriff, Admin Portale, etc.) muss der Anwender ein besonderes personalisiertes Administrator-Konto nutzen,
sein „normales“ User-Konto bekommt diese Rechte nicht / kann nicht den entsprechenden Rollen zugeordnet werden.

Verwaltung geheimer Authentisierungsinformation von Benutzern

Die Zuordnung von geheimer Authentisierungsinformation wird über einen formalen Verwaltungsprozess gesteuert.

Die Zuordnung geheimer Authentisierungsinformationen wird in IT Manufactory GmbH über einen formalen Prozess gesteuert.
Diese werden in IT Manufactory GmbH nur verschlüsselt gespeichert.
Alle Mitarbeiter verwenden ein entsprechendes Passwort-Tool KeePassXC für die lokale Speicherung.
Die IT Manufactory GmbH verwendet das Passwort-Tool Bitwarden.

Die Pflicht die Passwort Tools in allen Fällen zu verwenden ist durch entsprechende Richtlinien festgelegt.

Entzug oder Anpassung von Zugangsrechten

Die Zugangsrechte aller Beschäftigten und Benutzer, die zu externen Parteien gehören, auf Information und informationsverarbeitende Einrichtungen werden bei Beendigung des Beschäftigungsverhältnisses,
des Vertrages oder der Vereinbarung entzogen oder bei einer Änderung angepasst.

Bei Austritt werden Zugangsrechte und Rollen entzogen. Angestoßen wird dies über die Personalverwaltung.
Bei Beendigung einer Partnerschaft regelt der Partnermanager die Schließung der Zugänge.

Informationszugangsbeschränkung

Zugang zu Information und Anwendungssystemfunktionen ist entsprechend über Berechtigungen und Zugangssteuerungsrichtlinie eingeschränkt.

Die Zugangssteuerung wird über rollenbasierte Gruppen und entsprechende Gruppenzugehörigkeiten festgelegt und eingeschränkt.
Die benötigten Rechte werden über die jeweiligen Rollen bedarfsorientiert zugeteilt.

<u>Grundlegend gilt:</u>

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

Sowohl die Richtlinie, das Einhalten der Zugangssteuerung, als auch die Rollen und deren Rechte werden regelmäßig mindestens einmal pro Jahr überprüft.

<u>Für den Cloud-Betrieb gilt zusätzlich:</u>

Wir stellen sicher, dass bei der (Neu-) Vergabe von Speicherplatz dieser nicht mit Altdaten versehen ist.

Kryptographische Maßnahmen

<u>Wir betreiben folgende kryptografische Systeme:</u>

- Data Encryption Standard (DES),
- Asymetrische Kryptosysteme (Public Key) und
- Homomorphe Verschlüsselung.

Alle Daten werden mittels Kryptografiedienste verschlüsselt. Der / die ISMS-Beauftragte betreibt ein Programm zur Verschlüsselung. Alle Anwender/-innen werden in die Kryptografiedienste eingewiesen.

Daten die nicht kryptografisch verschlüsselt sind, werden dem / der ISMS-Beauftragte(n) mitgeteilt. In der Regel wird der auf dem Rechner installierte Stammdienst verwendet.

Der / die ISMS-Beauftragte prüft quartalsweise die Regelungen.

Schlüsselverwaltung
Eine Richtlinie zum Gebrauch, zum Schutz und zur Lebensdauer von kryptographischen Schlüsseln ist entwickelt und wird über deren gesamten Lebenszyklus umgesetzt.
Richtlinien zum Gebrauch, zum Schutz und zur Lebensdauer von kryptographischen Schlüsseln existieren und werden über deren gesamten Lebenszyklus umgesetzt.

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

- Benutzer: IT-Manufaktur-Entwicklungsteam, DevSecOps-Team
- Systeme: Der Zugang zu allen Servern (intern und extern) wird über SSH-Schlüssel verwaltet. DevSecOps ist dafür verantwortlich, den Zugang zu diesen Systemen für jeden Benutzer zu verwalten. Die Benutzer erhalten nur bei Bedarf Zugang zu den Systemen.
- Anwendungen: Entwickler sind angehalten, über ihre SSH-Schlüssel auf IT Manufactory Gitlab zuzugreifen.

Bestandsaufnahme der Vermögenswerte:

Die Sammlung aller SSH-Schlüssel und deren Zugriffsnutzung wird vom DevSecOps-Team auf Bitwarden gespeichert:

- In Bitwarden existiert ein spezieller Tresor mit einer Sammlung der öffentlichen SSH-Schlüssel aller Benutzer.
- Einzelne Benutzer können nur ihre Schlüssel in diesem Tresor einsehen. Zusätzliche Berechtigungen, um die Schlüssel anderer Benutzer einzusehen, können bei Bedarf von DevSecOps erteilt werden.
- Bitwarden speichert diese kryptographischen Schlüssel als eine sichere Notiz, und diese Schlüssel sind somit in verschlüsselter Form gespeichert.

Die Verwendung jedes Schlüssels, wie z.B. die zugehörigen Systeme und die Zugriffs-/Gewährungsebene, wird ebenfalls auf Bitwarden verwaltet. Wir haben auch alle aktiven, inaktiven oder widerrufenen Schlüssel für weitere Referenzen gespeichert.

SSH-Schlüsselgenerierungsrichtlinie:

Die Einrichtung des Entwicklers definiert die korrekte Art und Weise, ein SSH-Schlüsselpaar zu erstellen, das mit allen internen Konfigurationen kompatibel ist und gleichzeitig die Standard-

Sicherheitspraktiken einhält.
Alle SSH-Schlüsselpaare werden mit dem ECDH-Kurvenalgorithmus ED25519 erstellt.

Zugangsgewährung und -entzug:

Der rechtzeitige oder geplante Zugriff auf die Schlüssel wird von den DevSecOps-Teams verwaltet. Ein Benutzer kann ein standardmäßiges Jira-Ticket erstellen, um den Zugriff auf bestimmte Systeme zu gewähren. Die Anfrage des Benutzers wird dann ausgewertet, sein aktiver Schlüssel wird abgerufen und der Zugang wird dem Benutzer gewährt. Die Dauer des Zugriffs hängt von der jeweiligen Aufgabe und den Anforderungen des Benutzers ab.

Physische und umgebungsbezogene Sicherheit

Physischer Sicherheitsperimeter

Zum Schutz von Bereichen, in denen sich entweder sensible oder kritische Information oder informationsverarbeitende Einrichtungen befinden, sind Sicherheitsperimeter festgelegt und werden verwendet.

- Der Hauptsitz Passau wird durch elektronisches Zutrittskontrollsystem gesichert.
- Nur berechtigter Personenkreis hat Zutritt.
- Bereiche werden durch abgeschlossene Bereiche getrennt.
- Weitere Dokumentation finden sich unter der internen Dokumentation zur Zutrittskontrolle.

Physische Zutrittssteuerung

Sicherheitsbereiche sind durch eine angemessene nachvollziehbare Zutrittssteuerung geschützt, um sicherzustellen, dass nur berechtigtes Personal Zugang erhalten.

- Es gibt zwei Bereiche: nicht-öffentlicher Bereich und Sonderbereiche. Alle Zugänge sind gesichert und durch Schlösser mit AirKey versehen.
- Die Ausgabe, Übergabe und Rückgabe von Schlüsseln wird dokumentiert.
- Die Erstellung, Übergabe, Rückgabe und Vernichtung von AirKey wird dokumentiert und bei bedarf Gültigkeitszeiträume eingerichtet.
- Mitarbeiter werden im Zuge der Sicherheitsunterweisung auf den Umgang mit Gästen hingewiesen.
- Bei Verlust ist umgehend der ISMS Beuftragte zu informieren.

Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

Alle Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, werden überprüft, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind. Papier, Speichermedien und andere Geräte mit Informationen werden sicher vernichtet.

Die Entsorgung von Datenträgern ist so gestaltet, dass davon ausgegangen wird, es seien personenbezogene Daten enthalten:

- Experten des SecOps sammelt sie ein, vernichtet sie sicher vor Ort.

Die Vernichtung ist in der DIN 66399 beschrieben:

- Sicherheitseinstufung: vertraulich (DIN 66399-1)
- Securitylevel: Festplatten u. ä.: H-4 (DIN 66399-2), Papier: P-4 (DIN 66399-2)

Dies gilt auch für den Cloud-Betrieb.

Unbeaufsichtigte Benutzergeräte

Benutzer stellen sicher, dass unbeaufsichtigte Geräte und Betriebsmittel angemessen geschützt sind.

Die Richtlinien für die erneute Authentifizierungsaufforderung werden nach je Gerät unterschiedlich gehandhabt:

- Bei lokalem PC, bzw. Laptops, Notebooks nach 5 Min.
- Bei mobile Devices (Smartphones, Tablets, o.ä.) die PIN (bzw. Password, min. 4 Zeichen) und Speerzeit von 3 Min.
- Wechseldatenträger, mobile Geräte sind verschlossen aufzubewahren.

Siehe dazu auch die Arbeitssicherheitsrichtlinie als weiterführendes Dokument.

Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren

Die IT Manufactory GmbH lebt die Clean-Desk-Policy.

Richtlinien für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und für Bildschirmsperren für informationsverarbeitende Einrichtungen werden angewendet (Siehe auch 11.2.8 Unbeaufsichtigte Benutzergeräte).

Am Arbeitsplatz dürfen weder Unterlagen noch Datenträger mit sensiblen Daten unbeaufsichtigt und unverschlossen verbleiben.
Außerhalb der Arbeitszeiten sind sämtliche Dokumente mit sensiblen Daten, sowie mobile dienstliche Geräte der Mitarbeiter unter Verschluss zu halten.
Zugangsdaten (wie Username/Passwort) dürfen nicht schriftlich am Arbeitsplatz hinterlassen werden (etwa am Bildschirm angebracht, unter Tastatur oder Schreibunterlage – ausgenommen hiervon sind zentrale Administrations-Accounts,
die in entsprechenden Tools verwaltet werden). Vertrauliche Unterlagen und Unterlagen mit personenbezogenen Daten gehören NICHT in den Papierkorb, sondern sind entweder zu schreddern oder in Papierentsorgungs-Tonnen zu werfen.
Bildschirm, Post- und Ablagekörbe müssen so angebracht sein, dass kein Besucher im Vorbeigehen Einblick nehmen oder Unterlagen einstecken kann, ohne dass es auffallen würde. Im Falle von kurzen Abwesenheiten muss durch Abmelden von allen Systemen bzw. durch Sperren des Bildschirms (mit erneuter Passworteingabe) sichergestellt sein, dass niemand unberechtigten Zugang zu vertraulichen Daten erhält.

Beim Verlassen eines Besprechungszimmers sind alle Arbeitsdokumente, Präsentation, Flipcharts, Wechseldatenträger, etc. mitzunehmen.
Auch sind aus hygienischen Gründen alle Kaffeetassen- und Becher, Gläser, leere Flaschen, Geschirr und Unrat ordentlich zu entsorgen und der Tisch ist sauber zu hinterlassen.

Ausdrucke am Gemeinschafts-Drucker sind unverzüglich abzuholen. Bleiben Sie während des Druck- und Kopiervorgangs am Drucker bzw. Kopierer stehen.
Grundsäzlich wird Papierlos gearbeitet und nur in speziellen Fällen sollten ausdrucke und kopien gemacht werden.

Siehe dazu auch die Arbeitssicherheitsrichtlinie als weiterführendes Dokument.

Änderungssteuerung

Änderungen der Organisation, der Geschäftsprozesse, an den informationsverarbeitenden Einrichtungen und an den Systemen werden gesteuert und rechtzeitig mitgeteilt.

Alle Änderungen unterliegen dem Change Management Prozess und dieser steuert die jeweilige Änderung.
Gegebenenfalls werden Einweisungen durchgeführt oder Informationen erstellt.

Kapazitätssteuerung

Die Ressourcennutzung/Benutzung von Ressourcen wird überwacht und abgestimmt, und es werden Prognosen zu zukünftigen Kapazitätsanforderungen erstellt, um die erforderliche Systemleistung sicherzustellen.

Alle Ressourcen (IT-Infrastruktur, wie z.B. Netzwerk, Rechnerleistung, Speicher) werden regelmäßig geprüft.
Vorhersagen von System-Auslastungen und Auslastungs-Tendenzen werden über entsprechende Tools und Grafiken dargestellt und analysiert.

Planung von neuen Systemen, Systemerweiterungen und Leitungsupgrades werden im Rahmen von Projekten und in einem gesteuerten Change Management durchgeführt,
woraus wiederum entsprechende Maßnahmen zur Kapazitätserweiterung entstehen.

Grundsätzlich wird mit einem, der Dynamik der letzten Jahre angemessenen und den Prognosen über die weitere Entwicklung angepasstem, vorausschauenden Puffer geplant.

Trennung von Entwicklungs-, Test- und Betriebsumgebungen

Betriebsumgebungen sind voneinander strikt getrennt, um das Risiko unbefugter Zugriffe auf oder Änderungen an der Betriebsumgebung zu verringern.
Dafür werden eigene Betriebsumgebungen verwendet und rollenbasierte Zugangsdaten zur Verfügung gestellt.

Trennung für folgende Betriebsumgebungen:

- Entwicklung,
- Test,
- Marketing,
- Qualitätssicherung,
- Konsolidierung,
- Service,
- Schulung,
- Trail,
- Produktiv.

Dies ist durch entsprechende Prozesse gesichert.

Kunden Produktivsysteme sind nach Vertragsbestand Service Level Agreements (SLA) umgesetzt.

Dies betrifft insbesondere:

- Maßnahmen gegen Cyberangriffen,
- Früherkennung zu Notfällen,
- Vorbeugungs- und Wiederherstellungsmaßnahmen sowie
- die Sensibilisierung des bearbeitenden Personals.

Siehe dazu weiterführende Dokumentation der Datensicherungsrichtlinie und SLAs Wartungsverträge.
Wo IT Manufactory GmbH nicht die Entwicklung verantwortet (3rd Party Systeme) existieren ggf. keine Entwicklungssysteme. Trotzdem sind aber Qualitätssicherungs-/Konsolidierungs-/Testsysteme und Produktivsysteme auch hier strikt getrennt.

In Sonderfällen kann auch eine Umgebung zusätzlich weitere 2 voneinander getrennte Systeme umfassen (z. B. zwei getrennte Produktivsysteme für FirstCustomer Betrieb und Regelbetrieb, oder zwei getrennte Testsysteme, je eines für Smoketests und Implementierungstests).

Für den Cloud-Betrieb gilt zusätzlich:

IT Manufactory GmbH berücksichtigt die datenschutzrechtlichen Maßnahmen einschließlich Risikobetrachtung auch für Situationen, in denen Testdaten verwendet werden sollten.

Protokollierung und Überwachung

Ereignisprotokollierung

Über alle Vorkommnisse werden Protokollierungen durchgeführt und Ereignisse überwacht.

Dies erstreckt sich über:

- Ereignisprotokolle,
- Tätigkeiten von Benutzern und Administratoren,
- Ausnahmen,
- Störungen,
- Informationssicherheitsvorfälle.

Monitoring, Alerting und Protokollierung werden gesteuert durchgeführt. Sie sind im Applikationsmanagement verankert.

Die dazu gehörenden Richtlinien sind von IT Manufactory GmbH dazu im internen Atlassian Jira Confluence Operation festgelegt.

Für den Cloud-Betrieb gilt zusätzlich:

Nachverlangen bieten wir unseren Kunden die Möglichkeiten, relevanten Logdaten auszuhändigen. Die Regelmäßigkeit und Tiefe der Prüfung liegt dabei in der Verantwortung des Kunden.

Informationsübertragung

Richtlinien und Verfahren zur Informationsübertragung

Formale Übertragungsrichtlinien, -verfahren und -maßnahmen sind vorhanden, um die Übertragung von Information für alle Arten von Kommunikationseinrichtungen zu schützen.

IT Manufactory GmbH hat für die Übertragung von Daten (Data on the move) Regeln erlassen, wie damit umzugehen ist.

Entsprechende Verfahren und Maßnahmen dazu sind implementiert und werden angewendet. Siehe dazu auch die Informationen unter 13.2.3 Elektronische Nachrichtenübermittlung sowie 18.1.5 Regelungen bezüglich kryptographischer Maßnahmen.

Dies gilt auch für den Cloud-Betrieb.

Vereinbarungen zur Informationsübertragung

Vereinbarungen behandeln die sichere Übertragung von Geschäftsinformation zwischen der Organisation und externen Parteien.

Der Umgang mit der Übertragung von Daten (Data on the move) ist mit externen Partnern vereinbart.

Diese Vereinbarungen finden sich in den entsprechenden Verträgen:

- unter anderem in Non Disclosure Agreements (NDA),
- Lizenzverträgen für den Systemzugang (DA),
- den entsprechenden Servicebeschreibungen (die Vertragsbestandteil sind) oder individuellen Service Level Agreements (SLA) mit den Kunden.

Siehe zur technischen Umsetzung auch die Informationen unter 13.2.3 Elektronische Nachrichtenübermittlung.

Elektronische Nachrichtenübermittlung
Information in der elektronischen Nachrichtenübermittlung ist angemessen geschützt.
Alle Daten, die übertragen werden (Data on the Move), werden spätestens, wenn sie einen Zonenwechsel machen, verschlüsselt.
Die Verschlüsselung ist mindestens TLS 1.2 (mit AES 256 Bit).

Vertraulichkeits- oder Geheimhaltungsvereinbarungen
Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, werden identifiziert, regelmäßig überprüft und sind dokumentiert.

Vereinbarungen zur Geheimhaltung liegen vor sowohl für den internen als auch für den externen Einsatz.

Die Inhalte werden von Verantwortlichen (aus Recht, Datenschutz und Personal) verantwortet und regelmäßig gepflegt.

Quelle für Änderungen können sein u. a.: Audits, Gesetzgebung, Bedarfe im Austausch mit den Geschäftspartnern (Lieferanten, Kunden), Änderungen im Bestand schutzbedürftiger Werte.

Regelmäßiger Austausch im Umfeld Recht, ISMS und Datenschutz stellt die Beschäftigung mit den Vereinbarungen sicher.

<u>Inhalt der Geheimhaltungsvereinbarungen (NDA), auch wenn diese von der Gegenseite erstellt werden:</u>

- beteiligte Personen/beteiligte Organisationen,
- der Art der von der Vereinbarung umfassten Informationen,
- den Gegenstand der Vereinbarung,
- die Gültigkeitsdauer der Vereinbarung,
- den Verantwortlichkeiten des/der Verpflichteten.
- Geheimhaltungsvereinbarungen enthalten Bestimmungen zum Umgang mit den schutzbedürftigen Informationen über das Vertragsverhältnis hinaus. Ein Prozess, mit dem die Gültigkeitsdauer von befristeten
- Geheimhaltungsvereinbarungen überwacht und rechtzeitig eine Verlängerung der Geheimhaltungsvereinbarungen angestoßen wird, ist definiert und umgesetzt.

<u>Für den Cloud-Betrieb gilt zusätzlich:</u>

Kunden und Partner unterzeichnen bei Vertragsbeginn Standardverträge mit entsprechender Verpflichtung zur Geheimhaltung, auch in der Datenverarbeitung.
Mitarbeiter der IT Manufactory GmbH werden im Rahmen ihres Arbeitsvertrags auf Geheimhaltung verpflichtet und hierzu regelmäßig geschult.
Diese Verträge enthalten Zweckbindung entsprechend der Weisungsgebundenheit im Rahmen vorliegender Auftragsverarbeitung.
Die Pflicht zur Geheimhaltung geht über die Dauer der Vereinbarung hinaus.

Sicherheit in Entwicklungs- und Unterstützungsprozessen

Richtlinie für sichere Entwicklung

Regeln für die Entwicklung von Software und Systemen sind festgelegt und werden bei Entwicklungen innerhalb der Organisation angewendet.
Im Rahmen des SCRUM Prozesses ist die Berücksichtigung von Sicherheitsinteressen bei der Entwicklung und Pflege von Software und Systemen in Form von Prozessen und HowTos geregelt und definiert.
Für bestimmte Prozesse in der Softwareentwicklung sind Themenverantwortliche benannt.

Siehe dazu Agile Manifest als weiterführendes Dokument.

Verfahren zur Verwaltung von Systemänderungen

Die Umsetzung von Änderungen muss einem formalen Änderungskontrollverfahren unterliegen.
Die Umsetzungen von Änderungen wird im Rahmen eines Change Management durch Themenverantwortliche umgesetzt, welche die Release Planung und Kommunikation zum Kunden koordinieren
und Softwareveränderungen mit für Kunden bemerkbaren Auswirkungen bewerten.

Beschränkung von Änderungen an Softwarepaketen

Änderungen an Softwarepaketen werden nicht gefördert, sind auf das Erforderliche beschränkt, und alle Änderungen unterliegen einer strikten Steuerung. Im Rahmen des SCRUM Prozesses ist in Form von HowTos geregelt,
wie Softwareänderungen vor einer Freigabe zu bewerten sind. Die Steuerung der Änderungen unterliegt dabei themenverantwortlichen Produkt Managern.
Bei kundenindividuellen Systemen werden Änderungen auf Wunsch des Kunden durchgeführt.

Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme

Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme sind festgelegt, dokumentiert, werden aktuell gehalten und bei jedem Umsetzungsvorhaben eines Informationssystems angewendet.
Regeln, die Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme sicherstellen, finden sich in den entsprechenden Prozessen integriert, in den zugehörigen Anleitungen (HowTos) sowie übergreifend durch die Vorgaben des Security Guides und die Bereitstellung des Frameworks.

Sichere Entwicklungsumgebung

Organisationen schaffen sichere Entwicklungsumgebungen für Systementwicklungs- und Systemintegrationsvorhaben über den gesamten Entwicklungszyklus und schützen diese angemessen.
Die Bereitstellung, der Betrieb und die Pflege einer sicheren Entwicklungsumgebung ist durch entsprechende Themenverantwortliche sichergestellt. Sicherheit und Aktualität der Entwicklungsumgebung und der gesamten Applikationslandschaft werden dabei im Rahmen des Applikationsmanagements regelmäßig geprüft.

Ausgegliederte Entwicklung

Die Organisation beaufsichtigt und überwacht die Tätigkeit ausgegliederter Systementwicklung. Im Rahmen des Qualitätsmanagements ist in Form von Prozessen und HowTos geregelt und definiert, wie Tätigkeiten rund um ausgegliederter Systementwicklungen integriert und überwacht bzw. betrieben werden. Die Hauptverantwortung dafür trägt der jeweilige Partnermanager des jeweiligen Entwicklungspartners.

Testen der Systemsicherheit

Die Sicherheitsfunktionalität wird während der Entwicklung getestet.
Im Rahmen der Qualitätssicherung werden Neuentwicklungen manuell vor der Freigabe gegen die definierten Anforderungen sowie auf Anforderungen von Datenschutz und Sicherheit getestet.

Hierzu gibt es Testverantwortliche, welche das Testmanagement übernehmen. Zudem sichern automatische Tests kontinuierlich gegen unbeabsichtigte Seiteneffekte der Entwicklung ab.

Systemabnahmetest

Für neue Informationssysteme, Aktualisierungen und neue Versionen sind Abnahmetestprogramme und dazugehörige Kriterien festgelegt.

Im Rahmen des Qualitäts-, Change- und Release- Managements sind Prozesse und HowTos definiert, welche vorgeben, dass vor der Freigabe von neuen Informationssystemen, Aktualisierungen oder neuen Versionen entsprechende Abnahmen und Tests, geplant, und kontrolliert durch Themenverantwortliche, durchzuführen sind.

Regelmäßige Wartungsarbeiten (Software Wartung) werden teils weit im Voraus geplant und zusammen mit unregelmäßigen Wartungen dokumentiert.

Handhabung von Informationssicherheitsvorfällen und Verbesserungen

Verantwortlichkeiten und Verfahren

Handhabungsverantwortlichkeiten und -verfahren sind festgelegt, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sicherzustellen.

Der Prozess zur Sicherheitsvorfallmeldung ist organisiert und wird regelmäßig kommuniziert. Die Meldung erlaubt dazu mehrere Möglichkeiten zur Auslösung und wird toolgestützt prozessiert.

Mögliche Empfänger (etwa zu IT-Sicherheitsvorfällen, Datenpannen, Notfälle) sind durch Rollen verankert und geschult.
Näheres dazu unter 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation.

Für den Cloud-Betrieb gilt zusätzlich:

IT Manufactory GmbH hat einen internen Prozess zur Meldung und Behandlung von Sicherheitsvorfällen aufgesetzt.
Dabei wird u.a. die Kritikalität entsprechend den Sicherheitskriterien analysiert und im weiteren Vorgehen berücksichtigt.
Im Bedarfsfall sieht der Prozess vereinbarungsgemäß eine Zusammenarbeit mit den betroffenen Kunden vor.
Näheres dazu unter 6 Planung und Organisation der Informationssicherheit.

Meldung von Informationssicherheitsereignissen

Informationssicherheitsereignisse werden so schnell wie möglich an den Informationssicherheitsbeauftragten und Datenschutzbeauftragten gemeldet.

IT Manufactory GmbH hat Prozesse für Sicherheitsvorfälle implementiert, die sicherstellen, dass Informationssicherheitsereignisse so schnell wie möglich über geeignete, bekannte Kanäle zu deren Handhabung gemeldet und bearbeitet werden.
Dies umfasst sowohl Prozesse für den Regelbetrieb (den Sicherheitsvorfall und Incident Management) als auch für Ausnahmesituationen (Prozesse im Notfallmanagement sowie im Verfügbarkeitsmanagement oder zu Datenpannen im Datenschutz-Bereich).

Kunden können sich mit allen Sicherheitsanliegen und -meldungen an den IT Manufactory GmbH Service Management auf den ihnen jeweils zur Verfügung stehenden Kanälen wenden. Von hier werden erste Reaktionen aber auch Eskalationen ausgesteuert.

IT Manufactory GmbH meldet sich bei festgestellten eigenen Sicherheitsvorfällen umgehend bei den betroffenen Kunden.

Meldung von Schwächen in der Informationssicherheit
Beschäftigte und Auftragnehmer, welche die Informationssysteme und -dienste der Organisation nutzen, werden angehalten, jegliche beobachteten oder vermuteten Schwächen in der Informationssicherheit in Systemen oder Diensten festzuhalten und zu melden. Dies geschieht in einem Ticketing System Atlassian Jira Service.
Neue Mitarbeiter werden im On Boarding und bestehende Mitarbeiter in entsprechenden Schulungen auf die Mitwirkungspflicht hingewiesen. Kunden können sich mit allen festgestellten Schwachstellen an den IT Manufactory GmbH Customer Experience CX auf den ihnen jeweils zur Verfügung stehenden Kanälen wenden.
Von hier werden erste Reaktionen aber auch Eskalationen ausgesteuert.

IT Manufactory GmbH meldet sich bei festgestellten eigenen kritischen Schwachstellen umgehend bei den betroffenen Kunden.

Beurteilung von und Entscheidung über Informationssicherheitsereignisse
Informationssicherheitsereignisse werden beurteilt, und es wird darüber entschieden, ob sie als Informationssicherheitsvorfälle einzustufen sind.

Elementare Sicherheits -Vorfälle, -Ereignisse und -Gefärdungen:

- Ausfall oder Störung von Kommunikationsnetzen
- Ausfall oder Störung von Dienstleistern
- Fehlplanung oder fehlende Anpassung
- Offenlegung schützenswerter Informationen
- Informationen oder Produkte aus unzuverlässiger Quelle
- Manipulation von Hard- oder Software
- Manipulation von Informationen
- Unbefugtes Eindringen in IT-Systeme
- Ausfall von Geräten oder Systemen
- Fehlfunktion von Geräten oder Systemen
- Ressourcenmangel
- Software-Schwachstellen oder -Fehler
- Verstoß gegen Gesetze oder Regelungen
- Unberechtigte Nutzung oder Administration von Geräten und Systemen
- Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- Missbrauch von Berechtigungen
- Personalausfall
- Abstreiten von Handlungen
- Missbrauch personenbezogener Daten
- Schadprogramme
- Verhinderung von Diensten (Denial of Service)
- Sabotage
- Integritätsverlust schützenswerter Informationen

Reaktion auf Informationssicherheitsvorfälle
Auf Informationssicherheitsvorfälle wird entsprechend den dokumentierten Verfahren reagiert.

IT Manufactory GmbH hat Prozesse für Sicherheitsvorfälle implementiert, die sicherstellen, dass Informationssicherheitsereignisse so schnell wie möglich über geeignete, bekannte Kanäle zu deren Handhabung gemeldet und bearbeitet werden.

Dies umfasst sowohl Prozesse für den Regelbetrieb (den Sicherheitsvorfall und Incident Management) als auch für Ausnahmesituationen (Prozesse im Notfallmanagement sowie im Verfügbarkeitsmanagement oder zu Datenpannen im Datenschutz-Bereich).

Erkenntnisse aus Informationssicherheitsvorfällen

Aus der Analyse und Lösung von Informationssicherheitsvorfällen gewonnene Erkenntnisse werden dazu genutzt, die Eintrittswahrscheinlichkeit oder die Auswirkungen zukünftiger Vorfälle zu verringern.
IT Manufactory GmbH hat einen Prozess für Sicherheitsforfälle sowie einen Incident Prozess etabliert. Zu diesem gehört auch, dass sich um die Erkenntnisse aus Sicherheitsereignissen gekümmert wird und diese nachhaltig bearbeitet werden.
Gleiches gilt auch für das Notfallmanagement sowie Verfügbarkeitsmanagement oder die Bearbeitung von Datenpannen.

Regelmäßige Termine stellen die Auswertung und Beschäftigung mit Erkenntnissen sicher. Diese sind auch Input für das ISMS (etwa mit Blick auf Korrektur von Eintrittswahrscheinlichkeiten, Risikobewertung und Risikobehandlung).

Collection of evidence

Die Organisation legt die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Information, die als Beweismaterial dienen kann, fest und wendet diese an. Beweismaterial wird von der / dem ISMS-Beauftragte(n) verdichtet und aufgearbeitet. Die Geschäftsführung entscheidet, ob eine strafrechtliche Würdigung eingeleitet wird.

Beweismaterial:

- System Protokolle,
- Log Dateien,
- Notizen,
- Fotos von Bildschirminhalten
- Datenträger,
- Digitale Informationen,
- Personen
- Aktivitäten
- Sachverhalt

Compliance

Einhaltung gesetzlicher und vertraglicher Anforderungen

Das Risiko des Verstoßes gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Verpflichtungen mit Bezug auf Informationssicherheit wird betrachtet.

Privatsphäre und Schutz von personenbezogener Information

Die Privatsphäre und der Schutz von personenbezogener Information sind, soweit anwendbar, entsprechend den Anforderungen der relevanten Gesetze und Vorschriften sichergestellt.

Ein betrieblicher Datenschutzbeauftragter ist bestellt, der auf die Einhaltung der relevanten Datenschutzgesetze hinwirkt. Dieser kann auf den internen Syndikus oder einen externen RA für IT-Recht zurückgreifen.

Aus- und Weiterbildungsmaßnahmen zu diesen Themen und der Sicherstellung der Awareness sind für die Mitarbeiter eingerichtet.

Für extern kann ein Kontakt über unser Trust Center hergestellt werden.

Überprüfungen der Informationssicherheit

Die Informationssicherheit wird regelmäßig unternehmensübergreifend geprüft. Alle Abteilungen prüfen zusätzlich im eigenen Bereich die Informationssicherheit.

Die Ergebnisse fließen in die Informationssicherheitsbeurteilung ein.

Unabhängige Überprüfung der Informationssicherheit

Die Vorgehensweise der Organisation für die Handhabung der Informationssicherheit und deren Umsetzung werden auf unabhängige Weise in planmäßigen Abständen oder jeweils bei erheblichen Änderungen überprüft.

Wir unterziehen uns einer regelmäßigen externen Zertifikatsüberprüfung nach:

- Unabhängige Prüfung durch die Zertifizierer QM ISO 9001,
- Unabhängige Prüfung durch die Zertifizierer ISMS ISO 27001,
- Unabhängige Prüfung durch die Zertifizierer TISAX.

Überprüft werden:

- Maßnahmenziele,
- Maßnahmen,
- Richtlinien,
- Prozesse
- Verfahren

Die Ergebnisse werden in einem Auditbericht verdichtet. Derzeit halten wir eine jährliche Prüfung für ausreichend.
Zusätzlich wird durch die / den ISMS-Beauftragte(n) mit den Abteilungen besonders angesetzte Prüfungen durchgeführt bei Ereignissen und Vorfällen zur Informationssicherheit.

Weitere Prüfungen durch Dritte werden vorgenommen etwa zur Überprüfung der Datensicherheit:

- Überprüfung durch Kunden im Rahmen der Software -Integration und -Implementierung,
- Überprüfung durch Kunden im Rahmen von Security Self Assesments Fragen.

Teilweise können auch die Prüfungen der technischen und organisatorischen Maßnahmen (TOMs) gemäß Art. 28 DS-GVO durch unsere Geschäftspartner im Zuge Prüfungen zur Auftragsverarbeitung mit gewertet werden.

Für den Cloud-Betrieb gilt zusätzlich:

IT Manufactory GmbH bietet ihren Kunden vielfältige Informationen, um sich vom ordnungsgemäßen Betrieb zu überzeugen.
IT Manufactory GmbH lässt sich von unabhängigen, akkreditierten Stellen auditieren und stellt geeignete Belege wie Zertifikate zur Verfügung.

Einhaltung von Sicherheitsrichtlinien und -standards

Leitende Angestellte überprüfen regelmäßig die Einhaltung der jeweils anzuwendenden Sicherheitsrichtlinien, Standards und jeglicher sonstiger Sicherheitsanforderungen bei der Informationsverarbeitung und den Verfahren in ihrem Verantwortungsbereich.

Dazu haben wir ein mehrstufiges Konzept:

- Permanente Verantwortung und Prüfung durch die Rolle des Sicherheitsbeauftragten.
- Regelmäßige Meetings Informationssicherheit und technische Schulden.
- Regelmäßige interne Audits; mit Gegenprüfung der relevanten Sicherheitsrichtlinien und Stichproben-Tests.
- Regelmäßige Trainings zur Erinnerung und Auffrischung.
- Projektgetriebene Sicherstellung, dass die nötigen Aktivitäten laufen.
- Strategische Meetings wie Roadmap.

Überprüfung der Einhaltung von technischen Vorgaben

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

Dazu haben wir mehrere Situationen:

- Regelmäßige Tests im Rahmen des Change Managements durch IT-Operations.
- Permanente Verantwortung und Prüfung durch die Verantwortlichen der Leitlinien und die Rolle des Sicherheitsbeauftragten.
- Regelmäßige Überprüfung aus Datenschutz-Sicht durch den Datenschutzbeauftragten.
- Regelmäßige interne und externe Audits zur ISO 9001, ISO 27001, TISAX.
- Regelmäßige Termine im Informationssicherheit und technische Schulden Meeting.
- Regelmäßige Kontrolle und Pflege der Controls.

Leitfaden für Arbeitssicherheit

Der Leitfaden für die Arbeitssicherheit ist bereits in dem Dokument Arbeitssicherheit definiert.

Ort, den

Passau, 10.05.2022

Geschäftsführung