intech

Informationssicherheit

„White Paper“

Autor: Quixtner, Franz
(Chief Information Security Officer)

Lenkungsinformation

Gültigkeitsbereich: in-tech GmbH	**Version:** 3.0
Titel: Informationssicherheit "White Paper"	**Status:** Freigegeben
Schutzklasse: Intern	**Beteiligte Personen:** CISO

Änderungshistorie

Version	Inhalt	Autor, Datum	Freigeber, Datum
0.1	Initiale Erstellung	Franz Quixtner 05.03.2020	
0.2	<Im Entwurf> Designelement Deckblatt	Marketing 23.03.2020	
1.0	Inhaltliche Ausarbeitung und Freigabe	Franz Quixtner 26.03.2020	Dominik Rüdiger 03.04.2020
1.1	Design Anpassung	Franz Quixtner 09.11.2020	
2.0	Aktualisierung und Ergänzung bei 2.8	Franz Quixtner 19.03.2021	
2.1	Aktualisierung unter: 2.1 / 2.2 / 2.8 / 3.1 / 4.1 / 6.2 / 6.3 „Mobile Geräte“ (4.2) ergänzt	Franz Quixtner 29.09.2021	
3.0	Design Anpassung	Franz Quixtner 20.10.2021	

Inhalt

Vorwort

„Business Conduct“

Unser Leitbild beschreibt, welche Werte wir teilen und wie wir zusammenarbeiten wollen - heute und in der Zukunft. Es gibt uns ein klares Ziel vor, das es zu erreichen gilt, um unseren Erfolg nachhaltig zu sichern.

Wir können dieses Ziel nur gemeinsam erreichen. Hierbei spielen insbesondere unsere Werte wie persönliche Verantwortung, Offenheit und Transparenz sowie ein jederzeit gesetzeskonformes und ethisch korrektes Verhalten eine wichtige Rolle.

Die vorliegende Dokumentation führt unsere wichtigsten Grundregeln und Prinzipien an einer Stelle zusammen, diese sind für uns bereits heute gültig und auch in der Zukunft verbindlich. Es bietet uns einen Orientierungsrahmen und gilt für jeden von uns gleichermaßen - für die Geschäftsführung, für die Führungskräfte und für jeden einzelnen von uns. Es beschreibt unseren Anspruch an uns selbst, zugleich ist es auch ein Versprechen nach außen für unser verantwortungsvolles Handeln unseren Geschäftspartnern und der Öffentlichkeit gegenüber, aber auch im Umgang miteinander innerhalb des Unternehmens. Das Fehlverhalten eines Einzelnen kann für uns alle einen enormen Schaden verursachen.

Diese Richtlinie soll als Richtschnur für unser tägliches Handeln dienen.

„Zweck der Politik“

Unsere Unternehmenspolitik zur Informationssicherheit und Cybersicherheit beinhaltet unsere Richtlinien und Bestimmungen zur Wahrung der Sicherheit unserer Daten, Werte und unserer technischen Infrastruktur.

Je mehr wir uns bei der Erfassung, Speicherung und Verwaltung von Informationen auf Technologien verlassen, desto anfälliger werden wir für schwere Sicherheitsverletzungen.
Menschliche Fehler, Hackerangriffe und Systemfehlfunktionen könnten großen finanziellen Schaden verursachen und den Ruf unseres Unternehmens gefährden.

Aus diesem Grund haben wir eine Reihe von Sicherheitsmaßnahmen getroffen. Außerdem haben wir Anweisungen ausgearbeitet, die dazu beitragen können, Sicherheitsrisiken zu mindern.

„Umfang“

Die Maßnahmen, Richtlinien und Regelungen gelten für alle Mitarbeiter, Auftragnehmer, Besucher und alle, die dauerhaft oder vorübergehend Zugang zu unseren Systemen und unserer Infrastruktur haben.

1. Konformitätszertifizierung und -sicherung

Um einen strukturierten und strategischen Ansatz zur Informationssicherheit zu erreichen, führen wir unser Informationssicherheitsmanagementsystem in Übereinstimmung mit einer Reihe von bekannten Industriestandards durch. Wir wissen, dass diese Zertifizierungen und Labels besonders wichtig sind, da diese unseren Kunden eines erhöhten Informationssicherheitsstandard nachweisen und zudem eine unabhängige Sicherheit bieten.

STANDARD	BASIS	STATUS
ISO/IEC 27001:2017	**ISO/IEC** Internationale Organisation für Normung / Internationale elektrotechnische Kommission	Zertifizierte, Bereiche: Dienstleistungen für Entwicklung und Absicherung Elektrik / Elektronik Automotive, Industrie 4.0 und Transportation, Durchführung von Prüfungen und Tests am Fahrzeug, Durchführung von Prüfungen und Tests zur Qualitätssicherung, Entwicklung Entwicklung von Umrüstkits zur Elektrifizierung von Dieselfahrzeugen Entwicklung und Produktion von Ladekommunikationssteuergeräten, Beratung und Dienstleistung der Software, Entwicklung für Carsharing und Flottenmanagement Anbietern ISO/IEC 27001 nutzt auch die umfassenden Sicherheitsmaßnahmen, die in ISO/IEC 27002 detailliert beschrieben sind. Die Grundlage dieser Zertifizierung ist die Umsetzung eines Informationssicherheits-Managementsystems (ISMS).
TISAX®	**ENX Association** ist ein Zusammenschluss von Automobilherstellern, Zulieferern und vier nationalen Automobilverbänden	Information Security Assessment (ISA) des Verbandes der Automobilindustrie (VDA). Nachgewiesene Labels: Assessment Level **= AL3** ✓ Information with Very High Protection Level ✓ Connection to 3rd Parties with Very High Protection Level ✓ Data Protection with special categories of personal data ✓ Protection of Parts, Components and Prototypes

2. Verwaltung von Informationssicherheit

2.1 Informationsklassifizierung

Die in-tech Gruppe wendet die Informationsklassifizierung auf alle in der Organisation verwendeten Informationswerte an. Für diese identifizierten Werte (primäre, supportet oder Business Applikation Assets) werden gemäß dem CIA-Modell (**Vertraulichkeit**, **Integrität** and **Verfügbarkeit**) der Schutzbedarf ermittelt und entsprechend klassifiziert. Dies erfolgt in einem zentralen Wertemanagement (Asset-Management).

Stufe	Schutzbedarf	Klassifizierung
0	nicht relevant	Öffentlich
1	normal	Intern
2	hoch	Vertraulich
3	kritisch	Geheim

2.2 Informationssicherheits-Risikomanagement

Die in-tech Gruppe wendet das Informationssicherheitsrisikomanagement nach ISO27005 an, d.h. das systematische Erkennen und Bearbeiten von Risiken, wenn diese in Verbindung mit dem Verlust/Auswirkung auf die Vertraulichkeit, Integrität und/oder Verfügbarkeit eines Informationswertes hat.

Unser Ansatz für das Risikomanagement umfasst:

- Risikomanagement für die Informationssicherheit im Unternehmen - Wesentliche Änderungen an der Organisation, den Geschäftsprozessen oder den Informationsverarbeitungseinrichtungen, die die Informationssicherheit beeinflussen, werden durch einen Risikomanagementprozess gesteuert.
- Risikomanagement bei der Produktentwicklung - Das Risikomanagement für die Informationssicherheit wird als Teil unseres Produktentwicklungsrahmens angewandt.
- Risikobewertung im Projektmanagement – In der Planung und Durchführung von Projekten ist eine Risikoanalyse und -behandlung nach dem FEMA-Modell Standard.
- Risikomanagement für IT-Dienste/Systeme und Lieferanten - Die Anforderungen an die Informationssicherheit und die mit neuen IT-Systemen/Diensten sowie Lieferanten verbundenen Risiken werden durch einen Risikomanagementprozess innerhalb des Change-Managements kontrolliert.
- Risikomanagement und DSFA - Wenn die Verarbeitung personenbezogener Daten wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen, wird eine Datenschutzfolgenabschätzung (DSFA) durchgeführt, um einen angemessenen Schutz personenbezogener Daten zu gewährleisten.

2.3 Überprüfung der Informationssicherheit

Die in-tech Gruppe führt kontinuierlich Audits durch, um die Einhaltung von Standards, Richtlinien, Controls, Best-Practice, Gesetzen und Vorschriften zu gewährleisten. Ein weiterer wichtiger Aspekt ist für uns die kontinuierliche Steigerung der Leistung und Reife damit zu erzielen.

Die Audits werden von internen sowie externen unabhängigen Auditoren durchgeführt:

- Internes Informationssicherheitsaudit (jährlich)
- ISO 27001-Zertifizierungsaudit (jährlich)
- TISAX® – Konformitätsaudit (bei Scope Änderungen am jeweiligen Standort bzw. alle 3 Jahre)

2.4 Vorfalls-Management

Alle Informationssicherheits- und Datenschutzvorfälle werden von der Informationssicherheit- und Datenschutzorganisation gemäß den festgelegten Richtlinien und Verfahren verwaltet.

Das Meldewesen ist definiert und wird jährlich in unserer Informationssicherheitsschulung aufs Neue kommuniziert und erläutert.

2.5 Lieferantenmanagement

Um die erforderliche Einhaltung von Informationssicherheit und Datenschutzgesetzen zu gewährleisten, sowie die Merkmale der Dienstleistung aufrechtzuerhalten, werden dazu entsprechende Vereinbarungen getroffen und anschließend fortlaufend überwacht (Lieferantenaudit).

Zusätzlich pflegen wir einen „**Business Partner Code of Conduct**“ mit unseren Partnerfirmen (Lieferanten) zur Anerkennung unseres Verhaltenskodizes.

2.6 Leitlinien, Richtlinien und Vorgaben

Unser ISMS ist so strukturiert und aufgebaut, dass alle Bereiche der ISO-Norm und andere Regelwerke, denen wir nachkommen, abdeckt sind. Unser ISMS und die Verwaltung der Richtlinien soll sicherstellen, dass alle Vorgaben wie folgt:

- für alle relevanten Interessengruppen zugänglich ist
- an alle Mitarbeiter kommuniziert ist
- von der Geschäftsleitung genehmigt wurde
- Dokumentiert und leicht verfügbar ist
- die Definition der Sicherheitsziele einhält
- Engagement zur Erfüllung unserer regulatorischen Verpflichtungen zeigen
- auf kontinuierliche Verbesserung ausgerichtet ist
- Jährlich überprüft wird

2.7 Business Conduct

Unser Leitbild beschreibt, welche Werte wir teilen und wie wir zusammenarbeiten wollen - heute und in der Zukunft. Es gibt uns ein klares Ziel vor, das es zu erreichen gilt, um unseren Erfolg nachhaltig zu sichern.

Wir können dieses Ziel nur gemeinsam erreichen. Hierbei spielen insbesondere unsere Werte wie persönliche Verantwortung, Offenheit und Transparenz sowie ein jederzeit gesetzeskonformes und ethisch korrektes Verhalten eine wichtige Rolle.

2.8 Awareness für Informationssicherheit

Die in-tech Gruppe schult, trainiert und testet jährlich alle Mitarbeiter in Bezug auf die geltenden Richtlinien, Verfahren und Maßnahmen zur Sicherstellung der Informationssicherheit.

Nach Abschluss von Pflichtschulungen und bestandene Prüfungen der „**Informationssicherheitsschulung**“, „**Datenschutz**“, „**Unterweisung im Umgang mit Prototypen**“, „**Awareness Ransomware**“ oder „**Awareness Phishing Mails**“ erhalten die Mitarbeiter ein Sicherheitszertifikat.

2.9 Mitarbeiter GHV/NDA

Alle unsere Mitarbeiter unterliegen Vereinbarungen zur Informationssicherheit und Geheimhaltungsvereinbarungen.

3. Sicherheit in der Anwendung

3.1 Zugriffskontrolle

Die Zugriffskontrollen sind rollenbasiert und auf eine Need-to-know-Basis beschränkt. Jedem unserer Benutzer wird eine eindeutige Benutzer-ID zugewiesen, um die Integrität zu gewährleisten. Die eindeutige Benutzer-ID gilt für alle Mitarbeiter, einschließlich der Systemadministratoren und Systemaccounts.

in-tech GmbH verfügt über Prozesse, die Zugriffsrechte unmittelbar nach einer Änderung des Beschäftigungsstatus oder der Position eines Mitarbeiters zu ändern oder zu widerrufen. Zusätzlich dazu werden Berechtigungsreviews der Zugriffskontrolle durchgeführt.

3.2 Multi-Faktor-Authentifizierung

Für den Zugriff auf interne Services wird eine „starken Authentifizierung“ (bzw. Multi-Faktor-Authentifizierung) durchgesetzt.

3.3 Passwortrichtlinie

Alle Mitarbeiter oder Systemanwender der in-tech Gruppe haben individuelle Benutzerkonten und müssen mindestens mit Benutzername und Passwort authentifiziert werden. Zudem verfügen wir über eine Passwortrichtlinie deren Vorgaben 1zu1 technisch umgesetzt wird, um komplexe und sichere Passwörter sicherzustellen.

Die Passwort-Richtlinie kann an spezifische Kundenanforderungen angepasst werden.

Das Zurücksetzen des Passworts erfolgt nur im 4-Augen-Prinzip mit Authentifizierung einer zusätzlichen Führungskraft. Dazu haben wir eine separate technische Umsetzung mit einem Selfservice.

3.4 Clean Desk und Clear Screen

Mit unserer in-tech weiten Clear Desk / Clear Screen Policy verringern wir das Risiko des unberechtigten Zugriffs, des Verlusts von Informationen und des Schadens an Informationen während und außerhalb der Arbeitszeit.

Der Umgang mit Papieren und Speichermedien wie auch eine Sichere Datenvernichtung (Zertifizierte Aktenvernichtung und Löschverfahren nach den Empfehlungen des BSI) sind definiert und geregelt.

Der Umgang mit Papierausdrücken ist geregelt und nur mit Print2me möglich.

Automatisches sperren der Screens wie auch das automatische Abmelden an Systemen ist technisch umgesetzt.

3.5 Umgang mit Informationswerten

Die Informationswerte des Kunden werden für jeden Mandanten logisch getrennt, um die Vertraulichkeit und Integrität zwischen den Mandanten zu gewährleisten.

Diese Daten werden gemäß unserer Informationsklassifizierung eingestuft. Dies stellt sicher, dass alle relevanten Werte erfasst und klassifiziert und Regeln für den Umgang mit ihnen festgelegt und eingehalten werden. Zur Festlegung des jeweiligen Schutzbedarfs nach den Kriterien Vertraulichkeit, Integrität sowie Verfügbarkeit, ist ein Bewertungsschema in unserer Assetvorlage hinterlegt.

Der Zugang zu sensiblen Informationen wird nur nach dem Need-to-know-Prinzip vergeben.
Der Zugriff auf vertrauliche Informationen ist Teil der jährlichen Überprüfung der Rollenberechtigungen.

3.6 Ereignisprotokolle

Sofern technisch möglich, werden alle relevanten Aktivitäten innerhalb von Business Applikationen protokolliert. Diese Protokolle können Informationen über den Benutzer, Zeit und Datum, Benutzeraktivitäten und kritische Sicherheitsereignisse (wie z.B. Authentifizierungsversuche, die gegen die Regeln der Authentifizierung verstoßen) enthalten.

Um die Integrität dieser Protokolle vor Manipulationen zu schützen, werden die Zugriffsrechte auf die Quell-Protokolle streng begrenzt. Zusätzlich werden relevante Protokolle auf einem Syslog-Server zusätzlich gespeichert.

Die System- und Anwendungszeit wird mittels Network Time Protocol (NTP) synchronisiert.

3.7 Verschlüsselung

Die Kommunikation zwischen Endbenutzer und den in-tech Servern wird über die branchenüblichen Best-Practice-Verfahren verschlüsselt. Zudem sind alle mobilen Endgeräte (OS) verschlüsselt. Des Weiteren sind entsprechende der Einstufung der Informationsklassifizierung weitere technische Maßnahmen umgesetzt. Dies beinhaltet z.B. Content-Verschlüsselung, S/MIME, uvm.

4. Sicherheit des IT-Betrieb

4.1 Zugriffskontrolle

Der privilegierte Zugriff auf IT-Infrastrukturwerte wie Server, Switche, Firewalls usw. werden zusätzlich durch beschränkte Netzwerksegmente und einer Multi-Faktor-Authentifizierung geschützt.

4.2 Mobilgeräte

Mobilgeräte, wie etwa Laptops, Smartphones und Tablets, spielen mitunter eine wichtige Rolle bei der Erreichung unserer Unternehmensziele. Sie bergen jedoch auch beträchtliche Sicherheitsrisiken: So könnte ein Verlust/Diebstahl dazu führen, dass Unbefugte sich über diese Mobilgeräte unter Umständen Zugriff auf die IT-Infrastruktur der in-tech GmbH verschaffen.

Aus diesem Grund kommt dieser Regelung besondere Beachtung zu, um unsere Informationswerte zu schützen, Kundendaten und Zugänge abzusichern und unsere Reputation bewahren.

Deshalb sind unsere Endgeräte...

- zentral verwaltet
- deren Datenträger verschlüsselt
- personenbezogen Zugeordnet (keine Anmeldung weiterer MA möglich)
- durch eine starke Authentifizierung geschützt
- der Umgang bis hin zur Entsorgung geregelt und beschrieben

4.3 IT-Infrastruktur - Event logs

Event logs von diesen IT-Infrastrukturwerten werden zudem auf einer Syslog-Verwaltungsplattform gesichert, die vom IT-Team der in-tech Gruppe zentral verwaltet wird. Die Plattform wird zur Sammlung, Indizierung und Analyse von Syslog an einem zentralen Standort verwendet.

Die System- und Anwendungszeit wird mittels Network Time Protocol (NTP) synchronisiert.

4.4 Backup

Bei der in-tech Gruppe liegt ein Backupkonzept vor, das die internen Daten wie auch die jeweiligen Projektdaten des Kunden je nach Schutzbedarf entsprechend sichert und überwacht.

Im Konzept werden alle Sever-Systeme, Firewalls und Switch-Konfigs beachtet. Die täglichen Backups stehen mindestens zwei Woche lang zur Wiederherstellung zu Verfügung. Zudem stehen monatliche wie jährliche Sicherungspunkte zur Verfügung. Sicherung der aktuellen Backup-Daten in einem zweiten Brandabschnitt.
Backup-Wiederherstellungstests sind organisiert.
Recovery Time of Objektive und Recovery Point Objektive sind festgelegt und dokumentiert.

Als ergänzende Ransomware-Schutzmaßnahme wird ein Offline-Backup betrieben.

4.5 Schwachstellenmanagement

Bei der in-tech Gruppe ist ein Schwachstellenmanagement dokumentiert. Nach diesem sind mögliche Informationsquellen und Meldestellen festgelegt. Zudem liegt ein Software- und Patchmanagement vor, in diesem der Ablauf zu identifizierten Schwachstellen und Patches festgelegt und gemäß den internen Richtlinien und Verfahren klassifiziert, angewendet und behoben werden.
Die Systeme werden Systemgestützt überwacht und melden an definierte Überwachungsstellen.

4.6 Entwicklungsumgebung

Die in-tech Gruppe verfügt über getrennte Umgebungen für die Anwendungsentwicklung (Test / Integration / Produktiv).

5. Kommunikation und Netzwerksicherheit

5.1 Zugriffskontrolle und Authentifizierung

Die Anmeldung / Authentifizierung gegenüber Unternehmensnetzwerken mit Zugriff auf interne Ressourcen und Informationen erfolgt nur über VPN-Verbindung mit Multi-Faktor-Authentifizierung.
Webbased Services mit Zugriff auf Interne/Vertrauliche Daten ist ebenso nur über eine Multi-Faktor-Authentifizierung möglich. Ergänzend ist die Anmeldung nur von freigegebener Geo-Location möglich.
Zugang zu Netzwerken und Netzwerkdiensten wird nur dem berechtigten Mitarbeiter bzw. Anwender genehmigt.

5.2 Redundanz

Die in-tech Gruppe verfügt über redundante Netzwerkanbindungen und die Möglichkeit, die Kommunikation im unwahrscheinlichen Fall eines Netzwerkausfalls entsprechend zu Routen bzw. umzuleiten.

5.3 Netzwerkverschlüsselung

Die gesamte Site-to-Site-Kommunikation innerhalb der in-tech Gruppe ist über VPN Tunnels verschlüsselt.
Sämtlicher VPN-Verkehr von außen in die in-tech Infrastruktur ist verschlüsselt.
Interner Verkehr von in-tech Clients zu Produktionsdiensten wird verschlüsselt umgesetzt.

5.4 Schutz vor Schadsoftware

Um unsere Information(en) (Werte, kunden- und personenbezogene Daten) und informationsverarbeitende Einrichtungen, vor Schadsoftware (Malware) zu schützen, setzen wir bei der in-tech Gruppe verschiedene Sicherheitsmaßnahmen um.

Hierbei konzentrieren wir uns bei der Herangehensweise auf die Prävention wie auch auf das Erkennen von Schadsoftware im Betrieb. (ATP, Anti Viren Systeme, Firewalls, Ransomware Awareness Schulungen, uvm.)
Abschließend haben wir aber ebenso Vorgehensweisen definiert wie wir im Notfall unsere Information(en) und informationsverarbeitende Einrichtungen schützen und Wiederherstellen können.

5.5 Netzwerktrennung / Segmentierung

Um ein ausreichend hohes Maß an Sicherheit im internen Netzwerk zu gewährleisten, haben wir Unternehmensweit ein definiert Netzwerksegmentierung. Dazu sind Serversysteme, VOIP, Clientnetzwerk, Management und viele weitere, voneinander getrennt bzw. in jeweilige Bereiche unterteilt.
Diese sind nur bedingt miteinander vernetzt und doch jeweilige Firewalls getrennt.

5.6 Firewalls

Unsere Knotenpunkte des unternehmensweiten Netzwerkes sind jeweils mit Firewalls besetzt.
Zentrale Einheiten stehen durch Hot-Standby Cluster vor Ausfall geschützt.

Die eingesetzten Firewalls bieten alle nicht nur die modernsten Next-Gen-Firewall Sicherheit, sondern auch Funktionen wie z.B.: Network Protection (IPSec/SSL, VPN, IPS, DoS) Web & Mail Protection (URL Filter, Application Control, 2x Antivirus Engines, Deep Learning Protection).

6. Physische Sicherheit

6.1 Sicherheit im Rechenzentrum

Die zentralen IT-Systeme befinden sich im primären Rechenzentrum. Dieses verfügt über eine Reihe unterschiedlicher physischer Sicherheitskontrollen und Sicherheitsstandards wie z.B.:

- Strenge physische Multi-Faktor-Zugangskontrolle
- Zugriffsprotokolle
- Dedizierte und verschlossene Serverschränke
- Sicherheitsalarme
- Kontrollen zur Branderkennung und -verhütung
- Klimakontrollsysteme und Alarme
- Notstrom
- Unterbrechungsfreie Stromversorgung
- Blitzschutz
- Redundante Netzwerke
- Videoüberwachung

6.2 Sicherheit Serverräume

Ergänzend zum primären Rechenzentrum verfügen wir für sensible informationsverarbeitende IT-Systeme an unterschiedlichen Standorten entsprechend gesicherte Serverräume. Diese ist durch mehrere Zugangskontrollen und einer Einbruchmeldeanlage abgesichert.
Ebenso verfügen diese über eine Unterbrechungsfreie Stromversorgung (USV) und einer Klimatisierung.

Damit schaffen wir eine große Geo-Redundanz, die zur wesentlichen Ausfallsicherheit beiträgt.

6.3 Sicherheit im Projektoffice oder Flächen

Die jeweiligen Projekt- oder Büroflächen der in-tech Gruppe sind jeweils durch Zugangskontrollen sowie durch EMA / Sicherheits- und Brandmeldeanlage geschützt. Die Zutrittsberechtigungen sind geregelt.

Die Sicherheit an den physischen Standorten der in-tech Gruppe wird gemäß der ISO27001 sowie TISAX® VDA Vorgaben für physische Sicherheit und der Sicherheitsrichtlinie für den Arbeitsplatz verwaltet.

Dokumentierte Standortgefährdungsbeurteilungen und Sicherheitskonzepte liegen vor.

7. Datenschutz

Ziel des Datenschutzmanagementsystems bei in-tech ist der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

Um sicherzustellen, dass die Verarbeitung personenbezogener Daten (pbDaten) im Einklang mit den geltenden Gesetzen und selbstauferlegten Verpflichtungen steht, pflegt die in-tech Gruppe ein unternehmensweites Datenschutzmanagementsystem und stellt dazu intern eine Stelle des Datenschutzbeauftragten zur Verfügung.

In diesem Datenschutzmanagementsystem ist auch eine Richtlinie zum Umgang und Aufbewahrung pbDaten im in-tech Umfeld implementiert. Der Zweck dieser Richtlinie ist es die Konformität interner Prozesse, IT-Systeme und Anwendungen durch Design und Standard sowie die Prinzipien der Datenminimierung und Speicherbegrenzung sicherzustellen.

Die Basis dazu bildet unser Assetmanagement der informationsverarbeitenden (u.a. pbDaten) IT-Systeme in diesem der Schutzbedarf im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit festgelegt werden.

Die zum Erhalt eines angemessenen Schutzniveau der pbDaten notwendigen Maßnahmen werden zusammen mit der Informationssicherheit definiert, umgesetzt und überwacht.