Unternehmensleitlinie für Informationssicherheit

Auszüge der aktuell gültigen Version vom 7. Februar 2023

Diese Unternehmensleitlinie beschreibt Politik und Strategie der Finatix GmbH bzgl. dem Thema Informationssicherheit. Ziel ist die Definition des Zwecks, der Ausrichtung, der Grundlagen und der grundsätzlichen Regeln für die Mitarbeiter der Finatix GmbH zur Informationssicherheit, die im Informationssicherheitsmanagementsystem dargestellt wird.

---

1 Geltungsbereich

Das Informationssicherheitsmanagementsystem (ISMS) und damit alle Informationssicherheitsrichtlinien gelten für das gesamte Unternehmen mit Sitz in Leipzig, Barfußgäßchen 12, für alle Mitarbeiter basierend auf den Kerngeschäftsprozessen rund um die Themen IT Beratung, Entwicklung von Softwareprodukten in Eigenverantwortung sowie Entwicklung von Software im Auftrag des Kunden.

Die Unternehmensleitlinie für Informationssicherheit sowie die Informationssicherheitsrichtlinien der Finatix GmbH werden in Confluence als ISMS verwaltet, veröffentlicht und von der Geschäftsleitung freigegeben. Die Richtlinien sind Aufforderung und Verpflichtung zu gesetzeskonformen Verhalten und verantwortungsbewusstem Umgang mit der Informationssicherheits-Infrastruktur der Finatix GmbH für alle, die diese Infrastruktur nutzen. Sie werden allen Mitarbeitern, Kunden, Partnern und ggf. weiteren Personen oder Einrichtungen, d.h. allen interessierten Parteien in geeigneter Weise zur Kenntnis gegeben.

1.1 Zertifizierter Bereich:

Entwicklung und Betrieb von Software-Anwendungen im Cloud-Umfeld.

1.2 Beschreibung der Tätigkeiten im zertifizierten Bereich:

- Entwicklung von Client-Server Anwendungen auf Basis gängiger Entwicklungsframeworks (Java Spring, Kotlin, C#/.NET, Angular, React, Vue.js u.a.)
- Aufsetzen und Orchestrieren von Cloud-Diensten auf gängigen Cloud-Plattformen oder Private Clouds (Amazon Web Services, Microsoft Azure, Google Cloud Plattform u.a.)
- Betrieb und technischer Support für Anwendungen, die auf Cloud-Plattformen oder on premise betrieben werden

- Entwicklung modularer Softwareanwendungen in Microservice-Architekturen, Entwicklung von Schnittstellen und Benutzeroberflächen
- Entwicklung von Datenanalyse-, Datenauswertungs- und Datenvisualisierungs-software (Business Intelligence, Data Science, Machine Learning, Artificial Intelligence)

1.3 Nicht umfasste Tätigkeiten im zertifizierten Bereich:

- Entwicklung von Hardware und Firmware
- Aufsetzen und Hosting von Cloud-Infrastrukturen (eigene Cloud)
- Support und Sicherstellung der Verfügbarkeit von Cloud-Plattformen

2 Interessierte Parteien

Interessierte Parteien der Finatix GmbH sind:

- Gesellschafter
- Geschäftsleitung
- Kunden
- Lieferanten
- Mitarbeiter
- Gesetzgeber
- Behörden ohne BSI, BNetzA
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Bundesnetzagentur (BNetzA)
- Geschäftspartner

…

2.3 Weitergabe der Richtlinien an externe Geschäftspartner bzw. interessierte Parteien

Die als intern definierten Richtlinien der Finatix GmbH können bei Bedarf und fallbezogen (ggf. auch in Auszügen) an externe Geschäftspartner weitergegeben werden. Die Weiterleitung erfolgt immer direkt über den Informationssicherheitsbeauftragten in Abstimmung mit der Geschäftsführung. Bei relevanten Änderungen der Richtlinien des ISMS werden interessierte Parteien und Mitarbeiter informiert.

3 Bedeutung der Informationssicherheit

3.1 Informationssicherheitspolitik: Informationssicherheit als unverzichtbare Grundlage der Geschäftsprozesse

Informationen gehören zum wichtigen Kapital der Finatix GmbH. Informationen liegen in unterschiedlicher Form vor: als Papier, E-Mail, als gesprochenes Wort oder KnowHow und insbesondere in digitaler Form in Verbindung mit informationsverarbeitenden IT-Systemen. Die Finatix GmbH ist somit als Dienstleister im IT Bereich auf moderne Informations- und Kommunikationstechnik angewiesen, um ihre Geschäftsprozesse durchzuführen, die Leistungen für Ihre Kunden zu erbringen und um mit Kunden und Geschäftspartnern zusammenarbeiten zu können. Somit sollten die informationsverarbeitenden IT Systeme immer verfügbar sein.

3.2 Erfüllung von Rechtsvorschriften und vertraglichen Anforderungen

Darüber hinaus bestehen Verpflichtungen zur Gewährleistung der Informationssicherheit aufgrund von Gesetzen, wie z. B. die DSGVO und durch vertraglichen Verpflichtungen gegenüber Kunden, Mitarbeitern und Lieferanten.

3.3 Bedeutung der Informationssicherheit

Dem Schutz der Informationen und der Informations- und Kommunikationsinfrastruktur der Finatix GmbH vor Missbrauch, Manipulation, Störungen sowie dem Schutz der gespeicherten und verarbeiteten Informationen vor Manipulation oder Ausspähen – kurz: der Informationssicherheit – kommt daher für die Finatix GmbH eine existentielle Bedeutung zu.

3.4 Richtlinien zur Informationssicherheit im Unternehmen

Die Nutzung des Potentials eines funktionierenden Informationssicherheits-managementsystems (ISMS) ist eine wichtige Aufgabe zur Erhaltung der Wettbewerbsfähigkeit und unterstützt die strategischen Ziele der Finatix GmbH bzgl. Informationssicherheit. Aus diesem Grund hat die Geschäftsleitung der Finatix GmbH gemeinsam mit dem Informationssicherheitsbeauftragten die nachfolgenden Punkte für den Umgang mit der Informationstechnik der Finatix GmbH beschlossen. Darüber hinaus finden sich im ISMS des Unternehmens eine Vielzahl von Richtlinien für die Sicherstellung der Informationssicherheit.

4 Informationssicherheitsziele und Maßnahmen zur Erhaltung der Informationssicherheit

Die Ziele der Informationssicherheit sind es, einen anhaltenden geschäftlichen Erfolg und einen kontinuierlichen Geschäftsbetrieb sicherzustellen. Daher erfolgt die Sicherstellung der Informationssicherheit im ureigenen Interesse der Finatix GmbH, aber auch im Sinne von deren interessierten Parteien, wie z B. Kunden, Mitarbeitern, Lieferanten und Geschäftspartnern.

Um Informationssicherheit in möglichst großem Umfang zu gewährleisten, ist das Management von angemessenen Sicherheitsmaßnahmen unter Berücksichtigung einer großen Bandbreite von Risiken erforderlich.

- Die Finatix GmbH schützt ihre eigene Arbeitsfähigkeit, Vertrauenswürdigkeit und Zuverlässigkeit: Schutz der Reputation
- Die Finatix GmbH schützt die **Vertraulichkeit** der verarbeiteten und gespeicherten Informationen ihrer Kunden, Geschäftspartner und Mitarbeiter.
- Die Finatix GmbH schützt vertrauliche Informationen wie z.B. Geschäftsprozesse, Vertragsdaten oder sonstige Geschäftsgeheimnisse.
- Die Finatix GmbH gewährleistet die **Verfügbarkeit** ihrer IT-Systeme, Programme und Informationen.
- Die Finatix GmbH schützt die **Integrität** ihrer IT-Systeme, Programme und Informationen.
- Die Finatix GmbH verhindert den Missbrauch ihrer IT-Systeme, Programme und Informationen vor zweckwidriger Nutzung bzw. Nutzung durch Unbefugte.

4.1 Schutzmaßnahmen

Die Schutzmaßnahmen umfassen

- technische Maßnahmen (Software, Hardware, Konfiguration),
- organisatorische Vorkehrungen (verbindliche Regeln und Vorgaben) und
- personelle Maßnahmen (Schulungen, Mitarbeiterauswahl)

Die Schutzmaßnahmen sind an verschieden Stellen im Unternehmen zu finden, definiert und müssen umgesetzt/beachtet werden.

5 Organisationsstruktur und Verantwortlichkeit

Das Erreichen, Erhalten und ständige Verbessern eines angemessenen Informations-sicherheitsniveaus erfordert ein kontinuierliches Engagement von allen mit der Informations-verarbeitung befassten Personen wie dem Management, den Mitarbeitern sowie den Administratoren.

…

6 Fortlaufende Verbesserung

Die fortlaufende Verbesserung des angestrebten Informationssicherheits- und Datenschutzniveaus wird durch eine kontinuierliche Überprüfung der Regelungen sichergestellt.

Die Unternehmensleitlinie zur Informationssicherheit wird in regelmäßigen Abständen auf ihre Aktualität und Wirksamkeit hin überprüft und gegebenenfalls angepasst. Im Besonderen wird die Unternehmensleitlinie für Informationssicherheit bei Änderungen der Bedrohungslage aufgrund aktueller Ereignisse oder der Einführung neuer Technologien in der Finatix GmbH überprüft und angepasst. Unabhängig davon erfolgt eine Überarbeitung der Unternehmensleitlinie inkl. aller Richtlinien im ISMS einmal im Jahr.

7 Schulung des Bewusstseins zum Thema Informationssicherheit

Die Geschäftsleitung sowie die verantwortlichen Mitarbeiter der Finatix GmbH stellen durch bewusstseinsbildende Schulungs- und Sensibilisierungsmaßnahmen sicher, dass neue eingestellte Mitarbeiter ebenso wie bereits beschäftigte Mitarbeiter auf die Einhaltung der Unternehmensleitlinie für Informationssicherheit und der damit einhergehenden Richtlinien hingewiesen werden.

In regelmäßigen Abständen (mindestens einmal jährlich) werden alle Mitarbeiter in Schulungen auf die Problematiken und Gefährdungen in Zusammenhang mit Informationssicherheit und Maßnahmen zum Schutz vertraut gemacht.

8 Maßregelungen

Die Geschäftsleitung sowie leitende Angestellte stellen sicher, dass die Richtlinien zur Informationssicherheit durch alle Mitarbeiter befolgt werden. Mitarbeiter, die gegen diese Richtlinien verstoßen, können mit angemessenen Sanktionen belegt werden. Schwerwiegende Verstöße gegen die Grundsätze der Informationssicherheit können zu Abmahnung oder fristloser Kündigung eines Mitarbeiters führen.