Informationssicherheits-Managementsystem Leitlinie V1.7 vom 11.12.2020

Vertraulichkeitsstufe: Öffentlich

MightyCare Solutions GmbH
Vilbeler Landstraße 255
D-60388 Frankfurt am Main

Tel.: +49 69 8509603-0
Fax: +49 69 8509603-79
info@mightycare.de
www.mightycare.de

Geschäftsführer:
Peter Rudolf, Oliver Menzel
USt-IdNr. DE163754046
HRB 72034 / AG FFM

Bankverbindung:
Sparkasse Bremen
IBAN: DE17 2905 0101 0082 1702 75
BIC/SWIFT-Code: SBREDE22XXX

Inhalt

1. Gleichstellungshinweis

Im folgenden Dokument wird für die Beschreibung von Aufgaben, Funktionen oder Rollen aus Vereinfachungsgründen die männliche Schreibweise gewählt. Mit der gewählten Schreibweise werden in diesem Dokument alle Geschlechter angesprochen, denen Aufgaben, Funktionen oder Rollen zugeordnet werden, ohne eine Wertung ihres Geschlechts, ihrer physischen oder psychischen Fähigkeiten, oder eine sonstige Wertung vorzunehmen.

2. Zweck, Anwendungsbereich und Benutzer

Diese ISMS Leitlinie ist die Definition des Zwecks, der Ausrichtung, der Grundlagen und der grundsätzlichen Regeln für das Informationssicherheits-Managementsystem (ISMS) auf Basis der ISO/IEC 27001:2013.

Die Geschäftsleitung der MightyCare Solutions GmbH verabschiedet hiermit folgende ISMS-Leitlinie.

Zielsetzung dieser Leitlinie ist die Definition des Zwecks, der Ausrichtung, der Grundlagen und der grundsätzlichen Regeln für das Informationssicherheits-Management im Hause der MightyCare Solutions GmbH.

Die MightyCare Solutions GmbH richtet Ihre Unternehmenspolitik darauf aus, Spezialist in den Kernkompetenzen Colocation, Cloud und Managed Services zu sein. So unterstützt die MightyCare Solutions GmbH ihre Kunden bei der optimalen Gestaltung ihrer Arbeitsprozesse.

Die MightyCare Solutions GmbH bietet ihren Kunden und Partnern eine flexible und bei Bedarf geo-redundante Cloud in einer erstklassigen Infrastruktur mit skalierbarem Aufbau und bester Qualität aus Deutschland.

Um diese Leistungen zu gewährleisten, ist die MightyCare Solutions GmbH in einem höchsten Maße zur Erfüllung der Geschäftsprozesse verpflichtet, und um mit nationalen und internationalen Kunden und Partnern zusammenarbeiten zu können, auf die Verfügbarkeit moderner Informations- und Kommunikationstechnik angewiesen.

Darüber hinaus bestehen Verpflichtungen zur Gewährleistung der Informationssicherheit aufgrund gesetzlicher Bestimmungen und vertraglicher Verpflichtungen gegenüber Projektpartnern, Mitarbeitern und Kunden.

Dem Schutz der Informations- und Kommunikationsinfrastruktur des Unternehmens vor Missbrauch, Manipulation, Störungen, dem Ausspähen vertraulicher Informationen usw. – kurz: der Informationssicherheit – kommt daher eine immer größere Bedeutung zu.

Aus diesen Grund hat die Geschäftsführung die nachstehenden Leitlinien für den Umgang mit der Informationstechnik des Unternehmens beschlossen.

Diese Leitlinien sind Aufforderung und Verpflichtung zu gesetzeskonformen Verhalten und zu einem verantwortungsbewussten Umgang mit der IT-Infrastruktur des Unternehmens und der Kunden.

Diese Leitlinien gelten für Mitarbeiterinnen und Mitarbeiter sowie Auszubildende, Trainees, Praktikanten, Diplomanden, Werkstudenten und geringfügig Beschäftigte (im Folgenden auch Mitarbeiter genannt) und alle Externen mit einer Funktion im Anwendungsbereich des Informationssicherheits-Managementsystems. Sie werden allen Mitarbeitern und den entsprechenden Externen in geeigneter Weise zur Kenntnis gegeben.

3. Begriffe und Abkürzungen

- **Vertraulichkeit:**
  - Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.
- **Integrität:**
  - Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten.
- **Verfügbarkeit:**
  - Eigenschaft, einer berechtigten Einheit auf Verlangen zugänglich und nutzbar zu sein.
- **Informationssicherheit:**
  - Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen

- **Informationssicherheits-Managementsystem:**
  - Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt.

4. Informationssicherheitsziele und Schutzmaßnahmen

Die MightyCare Solutions GmbH stellt sowohl die Einhaltung regulatorischer und gesetzlicher Anforderungen, als auch die unbedingte Ausrichtung an den betrieblichen Erfordernissen zur Einhaltung von Anforderungen aus Verträgen mit Mitarbeitern, Kunden und Kooperationspartnern in den Mittelpunkt der Informationssicherheit.

Die MightyCare Solutions GmbH schützt ihre Interessen, insbesondere die Arbeitsfähigkeit, die Vertrauenswürdigkeit und Zuverlässigkeit für Kooperationspartner und Kunden sowie das Ansehen in der Öffentlichkeit, auch und gerade in Bezug auf die IT-basierten Arbeits- und Kommunikationsmittel.

Basis des Informationssicherheits-Managementsystems stellt die Risikoanalyse dar. Sie basiert auf den Unternehmenswerten, deren möglichen Gefährdungen und der Wahrscheinlichkeit des Auftretens sowie den Auswirkungen dieser Gefährdungen. Die Risikoanalyse berücksichtigt sowohl gesetzliche Anforderungen wie auch kundenspezifische und interne Anforderungen. Die Kriterien der

Risikoanalyse werden im Einzelnen in der Methodik zur Risikoanalyse und Risikobehandlung beschrieben.

Die MightyCare Solutions GmbH hat einen Prozess für die Handhabung von Informationssicherheitsvorfällen implementiert, bekanntgegeben und lebt diesen.

Die nachfolgenden übergeordneten allgemeingültigen Ziele wurden durch die Geschäftsführung der MightyCare Solutions GmbH festgelegt:

Die MightyCare Solutions GmbH…

- …stellt die Verfügbarkeit von Systemen und Diensten bei der Produktentwicklung sicher.
- …schützt Integrität und Vertraulichkeit der erzeugten bzw. verwendeten Daten und Programme.
- …stellt den Schutz von Authentizität, Vertraulichkeit, Integrität, Verbindlichkeit und Verfügbarkeit von erhaltenen, erzeugten, verarbeiteten und gespeicherten Informationen, z. B. Dokumentation, Designspezifikation zu den eigenen Produkten, Quellcode eigener Produkte, Testdaten, Entwicklungs- und Testumgebungen und von Kunden bereitgestellte Anforderungen, Spezifikationen oder Testdaten sicher
- …prüft Korrektheit und Qualität eingesetzter Fremdsoftware.
- …schützt Gebäude, Räume, IT-Systeme vor unberechtigtem Zutritt oder Zugang.
- …vermeidet Verstöße gegen gesetzliche oder vertragliche Vereinbarungen.
- …erwartet eine hohe Verlässlichkeit des Handelns, auch in Bezug auf den Umgang mit Informationen (Verfügbarkeit, Vertraulichkeit, Integrität).
- …wahrt einen guten Ruf des Unternehmens in der Öffentlichkeit.
- …strebt einen möglichst störungsfreien Betrieb der IT-Systeme an, um eine hohe Verfügbarkeit der Informationsverarbeitung und der Daten zu gewährleisten. Bei einem Ausfall der Informations- und Kommunikationstechnik im Geschäftsablauf durch Sicherheitsmängel darf der Regelbetrieb nicht stark beeinträchtigt werden.
- …schützt die Integrität der IT-Systeme und Daten, um regulatorische und gesetzliche Anforderungen und Anforderungen aus Verträgen mit Mitarbeitern, Kunden und Kooperationspartnern zu erfüllen und die Zuverlässigkeit der Informationsverarbeitung zu gewährleisten.
- …schützt ihre IT-Systeme und Daten vor Missbrauch, zweckwidriger Nutzung und vor der Nutzung durch Unbefugte, um sich selbst, die Beschäftigten, Kunden, Partner und sonstige Dritte zu schützen.

- …schützt ihre IT-Systeme und Daten vor unberechtigtem Zugriff, um das Ausspähen von Daten zu verhindern.

- …wahrt die Persönlichkeitsrechte ihrer Mitarbeiter.

- …führt regelmäßige Audits zur Sicherstellung der Einhaltung der Anforderungen durch.

- …hat das Ziel, einen vollständigen Überblick über die Lage der Informationssicherheit im Unternehmen zu erlangen und damit eine risikoorientierte und betriebswirtschaftliche Steuerung der risikominimierenden Maßnahmen zu ermöglichen.

- …hat das Ziel, das Unternehmen in die Lage zu versetzen, Unternehmenswerte gleich welcher Art angemessen zu bewahren und zu schützen, unabhängig von dem IT-Sicherheits-Knowhow von Einzelpersonen.

- …hat das Ziel, jeden Mitarbeiter des Unternehmens durch Aus- und Weiterbildung in die Lage zu versetzen, gemäß seiner Rolle und Aufgabe an dem Schutz der Informationswerte aktiv mitzuwirken.

Die Maßnahmen zur Erreichung der Ziele umfassen sowohl technische und organisatorische Vorkehrungen, als auch für alle Mitarbeiter verbindliche Regeln und Vorgaben. Sie werden in Form von Leitlinien, Policies und Verfahrensanweisungen verfasst und an einer zentralen Stelle im Intranet hinterlegt. Sie sind zu befolgen.

Die Strategie wurde mit der Überlegung ausgearbeitet, alle zur Verfügung stehenden Ressourcen effizient zu nutzen. Es sollen alle Bereiche der MightyCare Solutions GmbH in die Lage versetzt werden, ihre Informationen mit den Möglichkeiten der modernen Technik und den Methoden der Informationssicherheit zu schützen.

5. Verantwortlichkeiten

Das Erreichen und das Erhalten eines angemessenen Sicherheitsniveaus erfordert ein kontinuierliches Engagement von allen an der Informationsverarbeitung und an deren Planung und Administration beteiligten Personen.

- **Die Geschäftsleitung** trägt die Gesamtverantwortung für die Informationssicherheit und insbesondere für die Risikoakzeptanz. Sie initiiert und koordiniert die entsprechenden Aktivitäten und sorgt für die nötige Priorität und Aufmerksamkeit für Fragen der Informationssicherheit. Die Geschäftsleitung ist insbesondere verantwortlich für die organisatorische Verankerung von Aktivitäten zur Etablierung, Erhaltung und Weiterentwicklung der Informationssicherheit (Informationssicherheitsprozess) sowie für die technische und personelle Ressourcen-Ausstattung für die Informationssicherheit und deren angemessene Einbettung in die Strukturen und die Hierarchie des Unternehmens.

- **Der Arbeitskreis Informationssicherheit** unterstützt die Geschäftsleitung bei der firmenweiten Koordinierung und Lenkung der Informationssicherheitsmaßnahmen. Er erarbeitet konkrete Vorschläge technischer und organisatorischer Art zur Verbesserung der Informationssicherheit.
  Er hat darüber hinaus die Aufgabe, die bestehende Informationssicherheit zu bewerten, neue Gefahren zu erkennen und die einzelnen Sicherheitsmaßnahmen so zu koordinieren, dass ein angemessenes Sicherheitsniveau mit möglichst geringem Aufwand erreicht wird.

- **Die IT-Verantwortlichen bzw. der Informationssicherheitsbeauftragte** (der technische Geschäftsführer und der ISMB) legen Maßnahmen fest, die aus ihrer Sicht zur Verbesserung und Erhaltung der Sicherheit in ihrem jeweiligen Wirkungsbereich ergriffen werden müssen. Sie reagieren außerdem eigenverantwortlich bei Verstößen gegen die und bei Nichtbeachtung von Sicherheitsvorgaben.

- **Die Administratoren** setzen in enger Abstimmung mit dem jeweiligen IT-Verantwortlichen die notwendigen technischen und organisatorischen Maßnahmen zur Absicherung der IT-Infrastruktur um. Sie erarbeiten konkrete Handlungsanweisungen für die Benutzer der IT-Infrastruktur auch in Bezug auf die Informationssicherheit. Sie sind aufgefordert, Vorschläge für die Verbesserung der Informationssicherheit dem Arbeitskreis bzw. den IT-Verantwortlichen zu unterbreiten.

- **Die Vorgesetzten mit Personalverantwortung** stellen sicher, dass die technischen und organisatorischen Maßnahmen zur Informationssicherheit in Bezug auf die ihnen unterstellten Mitarbeiter bzw. die in ihrem Verantwortungsbereich tätigen Nutzern umgesetzt werden.

- **Jeder Nutzer** trägt durch sein Verhalten zur Gewährleistung der Informationssicherheit bei und trägt damit Verantwortung für die Informationssicherheit. Jeder Nutzer wird individuell über die zur Verfügung stehenden Sicherheitsmaßnahmen und -mechanismen informiert und achtet darauf, sie konsequent anzuwenden. Zu diesem Zweck erhalten alle Mitarbeiter Informationen, Schulung und Betreuung im Umgang mit den IT-Systemen und in Hinblick auf die sie betreffenden Sicherheitsmechanismen.

6. Sanktionen

Mitarbeiter, die gegen diese Sicherheitsrichtlinie verstoßen, können mit angemessenen Sanktionen belegt werden.