deepcloud

INFORMATIONSSICHERHEITSPOLICE

ISMS MANAGER
DEEPCLOUD AG
Wittenbach

ID: DC021 - DE
Version : 1.1
Datum : 8.9.2021

Klassifikation Level C1 - Public

Abteilung Dokumentenkontrolle

Protokolländerungen

Datum	Version	Status (Entwurf/zur Überprüfung)	Autor	Description
27.8.2021	1.0	Final	CEO/ISMS Manager	Erste Fassung
8.9.2021	1.1	Genehmigt	ISMS Manager	Aktualisierte Einleitung und kleinere semantische Änderungen (nicht relevant für den Inhalt)

Überarbeitung und Genehmigung/Freigabe

Datum	Version	Revision/Genehmigung	Änderungs- und Genehmigungsberechtigter	Anmerkung
8.9.2021	1.1	Genehmigung	CEO	

Quellenangaben auf externe Dokumente

Datum	Version	Doc ID	Name und Beschreibung	Dokumentenname/Link

Quellenangaben auf interne Dokumente

Datum	Version	Doc ID	Name und Beschreibung	Dokumentenname/Link

Verteilerliste

Datum	Name	Dokumentenname/Link
20.9.2021	Public	-

1. Inhaltsverzeichnis

2. Einleitung

DeepCloud AG ("Unternehmen") betrachtet den Schutz der Daten und der Organisationsstruktur (technologisch und physisch) als primäres Ziel für die Sicherheit der Informationen und hat demzufolge ein *Information Security Management System* (im Folgenden "ISMS") eingeführt und so konzipiert, dass dieses stets auf dem neuesten Stand ist sowie die Einhaltung der folgenden Sicherheitsmassnahmen die erfüllt werden müssen.

1. **Vertraulichkeit**, Alle Informationen/Daten sind nur für berechtigte Personen und/oder Prozesse zugänglich
2. **Integrität**, Konsistenz der Datenbanken und deren gespeicherten Informationen vor unbefugten Änderungen zu schützen
3. **Verfügbarkeit**, Bereitstellung der benötigten Informationen/Daten für autorisierte Benutzer, wenn diese angefordert werden.
4. **Kontrolle**, Sicherstellung der Datenverwaltung die durch geprüfte und sichere Prozesse und Instrumente erfolgen
5. **Authentizität**, Gewährleistung einer zuverlässigen Informationsquelle
6. **Datenschutz**, Gewährleistung des Schutzes und der Kontrolle der personenbezogenen Daten

Die Produkte und Dienstleistungen, die das Unternehmen über seine technologische Infrastruktur anbietet, werden durch die im ISMS implementierten Sicherheitsniveaus garantiert, die Folgendes umfassen:

- Systemzuverlässigkeit für das Prozess- und Informationsmanagement
- Höchste Sorgfaltspflicht für das Unternehmensbild
- Vollumfängliche Einhaltung des Service Level Agreements wie mit den Kunden vereinbart
- Kundenzufriedenheit
- Einhaltung der geltenden Vorschriften und des internationalen Sicherheitsstandards

Das im Unternehmen implementierte ISMS entspricht den Anforderungen der ISO/IEC 27001:2013 Standard und den für die Informationssicherheit relevanten Gesetzen im Rahmen der Geschäftstätigkeit des Unternehmens.

3. Umfang

Diese Informationssicherheitspolice gilt für alle internen Mitarbeitenden und Drittparteien, die eine Rolle bei der Verwaltung von Informationen spielen, sowie für alle Prozesse und Ressourcen, die an der Planung, Umsetzung, Inbetriebnahme und kontinuierlichen Bereitstellung von Unternehmensdienstleistungen beteiligt sind.

4. Geltungsbereich

Der Begriff "Sicherheit" wird im Unternehmen sehr weit gefasst und beinhaltet den Verlust von materiellen und immateriellen Vermögenswerten wie Informationen sowie Risiken im Zusammenhang mit der Unternehmenskontinuität. Das eingeführte ISMS wurde entwickelt, um solche Risiken frühzeitig zu erkennen und zu verhindern.

Der Mehrwert der vom Unternehmen verfolgten Informationssicherheitspolice liegt in ihrer Fähigkeit zu reagieren, bevor ein schädliches Ereignis eintritt. Dies ist möglich, weil jedes Mitglied der Organisation mit einer objektiven Vernunft handelt und seine Erfahrung einsetzt, um ein hohes Mass an Effizienz und Effektivität bei der Verwaltung der Informationssicherheit zu erreichen.

Die Informationssicherheitspolice des Unternehmens orientiert sich an folgenden Grundsätzen:

- Gewährleistung der vollständigen Kenntnisse der verwalteten Informationen und der Bewertung ihrer Kritikalität durch die Organisation, um die Umsetzung eines angemessenen Schutzniveaus zu vereinfachen
- Gewährleistung eines rechtmäßigen und sicheren Zugangs zu Informationen, um eine unbefugte Verarbeitung zu verhindern
- Scherstellung, dass die Organisation und Drittparteien bei der Verarbeitung von Informationen zusammenarbeiten, indem sie Verfahren einführen, die auf die Einhaltung eines angemessenen Sicherheitsniveaus abzielen
- Sicherstellung, dass die Organisation und Drittparteien, die an der Verarbeitung von Informationen beteiligt sind, sich der Sicherheitsfragen vollumfänglich bewusst sind
- Sicherstellung, dass Anomalien und Vorfälle, die das Informationssystem und die Unternehmenssicherheit betreffen, sofort erkannt, dokumentiert und durch effiziente Präventions-, Kommunikations- und Reaktionssysteme korrekt gehandhabt werden, um die Auswirkungen auf das Geschäft zu minimieren
- Sicherstellung, dass der Zugang zu den Büroräumlichkeiten und den einzelnen Firmengebäuden ausschließlich durch befugtes Personal erfolgt, um die Sicherheit der Bereiche und der entsprechenden Vermögenswerte zu gewährleisten
- Gewährleistung der Einhaltung der gesetzlichen Vorschriften und der in den Verträgen mit Drittparteien festgelegten Sicherheitsverpflichtungen
- Gewährleistung der Erkennung von anomalen Verhalten, Ereignisse und Schwachstellen von Informationssystemen, um die Sicherheit und Verfügbarkeit von Diensten und Informationen zu erhöhen
- Gewährleistung der Geschäftskontinuität und der Wiederherstellung im Fall eines gravierenden Zwischenfalles durch die Anwendung etablierter Sicherheitsverfahren

Die Informationssicherheitspolice ist im ISMS formalisiert, wird ständig aktualisiert, um ihre kontinuierliche Verbesserung zu gewährleisten, und wird der Organisation, Drittparteien und Kunden über die geeigneten Kommunikationskanäle mitgeteilt.

5. Zielsetzungen

In Übereinstimmung mit den oben genannten Grundsätzen definiert das Unternehmen die folgenden Zielsetzungen, die in allen Geschäftsprozessen verfolgt werden müssen:

- Verwaltung der Informationssicherheit, Definition angemessener Ziele, Bereitstellung geeigneter Ressourcen, Vorbereitung spezifischer Sicherheitsrichtlinien und -verfahren, die in den einzelnen Abteilungen implementiert werden sollen, wobei stets die vollständige Einhaltung gesetzlicher und regulatorischer Anforderungen sichergestellt wird
- Kommunikation von Informationssicherheitsstrategien, Zielsetzungen und Ziele, so dass ein wirklicher Austausch und eine Einigkeit über die zu ergreifenden Verhaltensweisen und Massnahmen bestehen
- Die Risikobedingungen zu minimieren und Schwachstellen zu vermeiden, um die Personen, Assets und das Unternehmen vor einer eventuellen Bedrohung zu schützen, sowie die

Unternehmensstandards, Zielsetzungen, Wettbewerbsfähigkeit, Marke und das Unternehmensbild zu gewährleisten

- Einbindung aller Mitarbeiter und Lieferanten durch Informations-, Bildungs- und Trainingsmassnahmen, die darauf anstreben, das Wissen, die Kompetenz und das Bewusstsein für die Aspekte der Informationssicherheit sowohl bei der Verwaltung der täglichen Aktivitäten als auch bei Vorfällen, die eine Geschäftskontinuität gefährden könnten, zu erhöhen
- Gewährleistung einer raschen Rückkehr zum Normalbetrieb bei Notfällen und Krisen, Einschränkung von Schäden und Verlusten, Schutz von Personen und Unternehmensvermögen
- Überwachung interner Prozesse zur ständigen Überprüfung der Angemessenheit des Systems und zur Ermittlung möglicher Verbesserungsmassnahmen
- Verbesserung des ISMS, um es an die sich ändernden globalen, geschäftlichen und gesetzlichen Anforderungen anzupassen

Die oben genannten Grundsätze und definierten Ziele sind fester Bestandteil der täglichen Arbeit des Unternehmens. Zur Erreichung dieser Ziele werden alle nötigen technischen, organisatorischen und operativen Massnahmen ergriffen und in einem kontinuierlichen Prozess überwacht und überprüft

6. Verantwortung für die Informationssicherheitspolice

Die Geschäftsleitung ist dafür verantwortlich, dass das ISMS stets auf dem neuesten Stand ist und der Entwicklung des Geschäfts- und Marktumfelds entspricht, indem sie alle Massnahmen bewertet, die in Bezug auf folgende Punkte basieren:

- Wesentliche Geschäftsentwicklungen
- Risikoanalyse von neuen Bedrohungsaktivitäten
- Relevante Sicherheitsvorfälle
- Änderungen im regulatorischen oder rechtlichen Kontext in Bezug auf die sichere Verarbeitung von Informationen

Die Verantwortung für den Schutz der Personen und der Unternehmensressourcen liegt bei der Organisation. Alle, die Unternehmensprozesse verwalten, betreiben und kontrollieren, müssen ein angemessenes Schutzniveau gewährleisten, indem sie die vom Unternehmen zur Verfügung gestellten Instrumente und Ressourcen nutzen.

Die Leiter der einzelnen Funktionen und Abteilungen müssen daher sicherstellen, dass diese Informationssicherheitspolice von allen Mitarbeitenden und den beteiligten Lieferanten verstanden und umgesetzt dementsprechend umgesetzt wird.