ISL_004_GF

Informationssicherheitspolitik

– Freigabe für extern und intern –

itsc GmbH
Rotenburger Str. 24
30659 Hannover

Telefon: 0511 27971-0
Web: itsc.de
E-Mail: info@itsc.de

Sitz der Gesellschaft: Hannover
Eingetragen beim Amtsgericht Hannover HRB 57 585

Inhaltsverzeichnis

1 Verantwortung

Die Geschäftsführung der itsc GmbH hält die Informationssicherheit für ein unverzichtbares Qualitätsmerkmal unserer Dienstleistungsprozesse. Die Einhaltung der notwendigen firmeninternen Informationssicherheitsrichtlinien gehört zu den elementaren Grundlagen der Firmenphilosophie. Alle Mitarbeiter des Unternehmens müssen die unabdingbare Notwendigkeit verstanden haben, um die täglichen Aufgaben auch in diesem Sinne durchzuführen.

Die Geschäftsführung unterstützt und fördert die dazu notwendigen Strukturen und Prozesse und hat Verantwortliche benannt, die diese Informationssicherheitspolitik in Verfahrensanweisungen, Arbeitsanweisungen und Dokumentationen umsetzen und im Tagesgeschäft verankern.

Die Geschäftsführung stellt die dazu erforderlichen Ressourcen in Form von Mitarbeiterkapazität und Geld zur Verfügung und verpflichtet sich, die Angemessenheit und Wirksamkeit des Informationssicherheitsmanagementsystems regelmäßig zu überprüfen und laufend zu verbessern.

2 Geltungsbereich

Die Regelungen der Bewirtungsrichtlinie gelten für alle Mitarbeitenden der itsc GmbH.[1]

3 Normative Referenzen

Die Grundlage für diese Richtlinie bildet die ISO/IEC 27001:2013 (im Folgenden: ISO 27001):

- 5.1 Führung und Verpflichtung
- 5.2 Politik
- Kap. 5.2 Politik

sowie den zugehörigen Dokumenten in der jeweils gültigen Version.

4 Zweck

Die itsc GmbH kommt als Digitalisierer, Systemintegrator und IT-Dienstleister täglich mit hochsensiblen Daten und Informationen ihrer Kunden in Berührung. Diese Informationssicherheitspolitik legt Grundprinzipien für die Gewährleistung der Sicherheit und Integrität dieser Daten und Informationen fest.

5 Sicherheitsziele

- Gewährleistung der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Daten der itsc GmbH und ihrer Geschäftspartner.
- Absicherung der Dienstleistungsprozesse transparent gestalten und durch eine etablierte Sicherheitsorganisation absichern.

[1] Wir verwenden im Dokument soweit möglich eine geschlechtsneutrale Sprache. Wo dies aus Gründen des guten Leseflusses ausnahmsweise nicht erfolgt, sind bei der Verwendung des generischen Maskulinums stets alle Geschlechter gemeint.

- Erkennung und Begrenzung von Informationssicherheitsrisiken auf ein akzeptables Maß.
- Verhinderung von Reputations- oder finanziellen Schäden durch den Verlust von Daten oder Informationen.
- Nachweis der Sicherheit der Organisation gegenüber Kunden, Gesetzgeber, Partnern, Versicherungen und Lieferanten.

6 Grundsätze

Die itsc GmbH schützt die Vertraulichkeit und Integrität von Kundendaten. Sie weist dies in einer Form nach, die es aktiven und potentiellen Kunden erleichtert, sich von der Angemessenheit der ergriffenen Maßnahmen zu überzeugen und die itsc GmbH als Dienstleister einzusetzen.

Die itsc GmbH führt regelmäßige Fortbildungen für Mitarbeiter zu Themen des Datenschutzes und der Informationssicherheit durch.

Daten und Informationen werden klassifiziert und mit Verfahren bearbeitet, die ihrer Klassifizierung angemessen sind.

Die itsc GmbH betreibt ein Risikomanagementsystem mit dem Ziel, Risiken für die Integrität, Sicherheit oder Vertraulichkeit von Daten und Informationen zu erkennen und auf ein akzeptables Maß zu begrenzen.

Die itsc GmbH betreibt ein präventives Notfallmanagementsystem mit dem Ziel, Risiken für die Verfügbarkeit von Daten und Informationen zu erkennen. Für den Notfall sind Prozesse etabliert, die die Verfügbarkeit schnellstmöglich wiederherstellen.

Veränderungen von Systemen und Anwendungen unterliegen einem definierten Change-Management-Prozess, der Aspekte des Datenschutzes und der Informationssicherheit berücksichtigt.

Die itsc GmbH verwendet ein Berechtigungskonzept, nach dem Mitarbeiter nur die Berechtigungen erhalten, die sie für ihre Arbeit benötigen.

Die itsc GmbH betreibt ihre Infrastrukturen mindestens nach dem Stand der Technik.

Durch regelmäßige interne Audits wird sichergestellt, dass die Vorgaben zum Datenschutz und zur Informationssicherheit von den Mitarbeitern umgesetzt und eingehalten werden und dass Schwachstellen erkannt und Verbesserungsmöglichkeiten genutzt werden.