Informationssicherheitspolitik der SVA System Vertrieb Alexander GmbH

SVA System Vertrieb Alexander GmbH
Borsigstraße 14
65205 Wiesbaden
Tel. 06122/536-0
www.sva.de

Titel:	Informationssicherheitspolitik	
Verantwortlicher Autor:	Jochen Guther	
Dateiname:	Informationssicherheitspolitik V2.pages	
Vertraulichkeitsstufe:	S1 - öffentlich	
Versionsnummer:	2	
Bearbeitungsstatus:	gültig	
Freigaben:	Name & Position	Datum
Version 1	Philipp Alexander	26.08.2016
Version 2	Philipp Alexander	21.11.2016

Versionsnr.	Status	Datum	Bearbeiter	Änderungen/Bemerkungen
0.1	Entwurf	29.4.2016	Jochen Guther	erster Versuch
0.2	Vorlage GF	15.6.2016	Jochen Guther	inhaltlich vervollständigt
0.3	Abstimmung GF	20.6.2016	Felix Alexander	Abschnitt „Verantwortung“ erweitert
1	Genehmigt GF	26.8.2016	Jochen Guther	Schreibfehler korrigiert und Unterschriftsblock ergänzt
2	Genehmigt GF	21.11.2016	Jochen Guther	ergänzt, welche Teile nur für SVA Operational Services gelten

Geltungsbereich

Die Informationssicherheitspolitik gilt für alle Standorte und Mitarbeiter der SVA System Vertrieb Alexander GmbH.

Verantwortung

Die Geschäftsführung der SVA 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.

Zweck

SVA kommt als Systemintegrator und IT-Dienstleister häufig 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.

Sicherheitsziele

- Vertraulichkeit, Integrität und Verfügbarkeit von Daten der SVA und ihrer Geschäftspartner gewährleisten
- Dienstleistungsprozesse transparent gestalten und durch eine etablierte Sicherheitsorganisation absichern
- Informationssicherheitsrisiken erkennen und auf ein akzeptables Maß begrenzen
- Reputations- oder finanzielle Schäden durch den Verlust von Daten oder Informationen verhindern
- Sicherheit der Organisation gegenüber Kunden, Gesetzgeber, Partnern, Versicherungen und Lieferanten nachweisen

Klassifizierung von Daten / Informationen / Dokumenten

SVA verwendet die folgenden Klassifizierungsstufen:

Stufe	Bezeichnung	Beispiel
S1	öffentlich	Marketing-Informationen
S2	vertraulich	Verträge, Bewerbungen
S3	geheim	besonders schützenswerte Personendaten, Geschäftsgeheimnisse

Grundsätze

- SVA führt regelmäßige Fortbildungen für Mitarbeiter zu Themen des Datenschutzes und der IT-Sicherheit durch.
- SVA schützt die Vertraulichkeit und Integrität von Kundendaten. Sie weist dies in einer Form nach, die es potentiellen Kunden leicht macht, sich von der Angemessenheit der ergriffenen Maßnahmen zu überzeugen und die SVA als Dienstleister einzusetzen.
- SVA verwendet ein Berechtigungskonzept, nach dem Mitarbeiter nur die Berechtigungen erhalten, die sie für ihre Arbeit benötigen.

Für den Geschäftsbereich SVA Operational Services gilt darüber hinaus:

- Daten und Informationen werden klassifiziert und mit Verfahren bearbeitet, die ihrer Klassifizierung angemessen sind.
- SVA betreibt ein Risikomangementsystem mit dem Ziel, Risiken für die Integrität, Sicherheit oder Vertraulichkeit von Daten und Informationen zu erkennen und auf ein akzeptables Maß zu begrenzen.
- Veränderungen von Systemen und Anwendungen unterliegen einem definierten Change-Management-Prozess, der Aspekte des Datenschutzes und der Informationssicherheit berücksichtigt.
- 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.

Wiesbaden, den 21. November 2016

Philipp Alexander
Geschäftsführer
SVA System Vertrieb Alexander GmbH