VINTIN GmbH
Felix-Wankel-Straße 4
D-97526 Sennfeld
Tel. +49 (0)9721 675 94 10
www.vintin.de

LEITLINIE FÜR DIE INFORMATIONSSICHERHEIT DER VINTIN

DATUM 26.07.2018

Informationssicherheitsleitlinie als Bestandteil der organisationsweiten Sicherheitsstrategie und auf Grundlage der Anforderungen aus der Norm ISO/IEC 27001.

INHALTSVERZEICHNIS

Inhalt

DOKUMENTEN-INFORMATION

Dokumenten-Information

PROJEKTNAME:	Einführung eines ISMS nach ISO/IEC 27001
TITEL:	Leitlinie für die Informationssicherheit der VINTIN
ERSTELLT DURCH:	Philipp Zacharias
VERSIONSNUMMER:	V1.6
VERSIONSDATUM:	26.07.2018
FREIGEGEBEN VON:	Philipp Zacharias
FREIGABEDATUM:	26.07.2018

Versionsverlauf

VERSION	VERSIONSDATUM	GEÄNDERT VON:	BESCHREIBUNG	STATUS
V1.0	04.04.2017	André Scherwinski	Erstellung	Entwurf
V1.1	21.04.2017	Daniel Baumgärtner	Anpassung Layout	Entwurf
V1.2	18.05.2017	Philipp Zacharias	Finalisierung	Final
V1.3	12.10.2017	Philipp Zacharias	Aktualisierung	Final
V1.4	19.10.2017	Philipp Zacharias	Korrektur	Final
V1.5	10.04.2018	Philipp Zacharias	Aktualisierung zur Veröffentlichung	Final
V1.6	26.07.2018	Philipp Zacharias	Aktualisierung	Final

Zielstellung

Die VINTIN Unternehmensgruppe vereint heute unter einem Dach fundierte Kompetenz in allen Bereichen der IT-Infrastruktur bis zur Cloud. Die Fachbereiche sind spezialisierte Ansprechpartner für individuelle Kundenbedürfnisse und bieten optimale Lösungen für Datennetzwerktechnik und IT-Security, klassische Systemhauslösungen wie Backup, Storage und Serverleistungen sowie moderne Lösungen von Managed Services über Cloud Computing bis hin zum kompletten Outsourcing der IT. Neben dem zentralen Standort in Sennfeld bei Schweinfurt unterhält die VINTIN Unternehmensgruppe Niederlassungen und Servicestützpunkte in Fulda, München, Leipzig und Malters (Schweiz).

Teil der VINTIN Unternehmensgruppe ist die VINTIN Services GmbH. Sie bietet als innovativer Cloud-Dienstleister moderne, anpassungsfähige und hoch skalierbare Cloud-Lösungen für alle Unternehmensgrößen und -bereiche an. Das Leistungsspektrum reicht von der Virtualisierung der Client-/Serverinfrastruktur und dem Neuentwurf der Netzwerkinfrastruktur, über deren Betrieb und Wartung, bis hin zur Benutzerbetreuung und -schulung.

Die Informationsverarbeitung (IV) stellt für die VINTIN Unternehmensgruppe einen essentiellen Bestandteil für die tägliche Arbeit dar. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt.

Weiterhin stellt die IV eine entscheidende Rolle für die Wettbewerbsfähigkeit in der Informations- und Telekommunikationsbranche dar. Die Lieferung innovativer und qualitativ hochwertiger Dienstleistungen und auch die Bereitstellung von einwandfreien und zuverlässigen Produkten, einschließlich des Nachweises über die Qualität und Sicherheit interner Prozesse, ist nicht nur eine Erwartung der Kunden, sondern stellt auch einen Wettbewerbsvorteil dar.

Die Geschäftsführung der VINTIN Services GmbH verabschiedet folgende Informationssicherheitsleitlinie als Bestandteil der organisationsweiten Sicherheitsstrategie und auf Grundlage der Anforderungen aus der Norm ISO/IEC 27001.

Die Geschäftsführung sieht sich in der Pflicht, Maßnahmen zur Informationssicherheit und zum Datenschutz in den Geschäftsprozessen zu implementieren und deren Wirksamkeit im Rahmen eines Informationssicherheitsmanagementsystems (ISMS) aufrecht zu erhalten und zu verbessern.

Grundsatz ist es, die Informationssicherheit in der gesamten Unternehmensgruppe aufrechtzuerhalten, zu verbessern und dem Kunden einen Mehrwert an Informationssicherheit zu bieten.

Geltungsbereich

Die Informationssicherheitsleitlinie gilt für die VINTIN Services GmbH und den im ISMS festgelegten Anwendungsbereich. Ziel ist es den Geltungsbereich auf die gesamte VINTIN Unternehmensgruppe zu erweitern.

Der Aufbau des Managementsystems bei der VINTIN Services GmbH soll als Musterbeispiel für die gesamte Unternehmensgruppe gelten.

ISMS-Anwendungsbereich

Das ISMS steuert die Informationssicherheit der Prozesse, Daten und Systeme im Zusammenhang mit der Leistungserbringung des Servicedesk des sicheren Betriebes. Damit werden die Dienstleistungen gegenüber den Kunden der VINTIN Services GmbH hinsichtlich der Verfügbarkeit, Vertraulichkeit und Integrität der Daten und Systeme positiv beeinflusst.

Anwendung findet das ISMS an den Standorten der VINTIN Services GmbH in Sennfeld und in Fulda. Wobei sich die Räumlichkeiten in Fulda in einer durch den Kunden bereitgestellten Lokation befinden. Der Anwendungsbereich des ISMS liegt konkret im Bereich der Service Operations und somit den Dienstleistungsservices und dem dazugehörigen Betriebsmanagement. Dazu zählen Office 365 und Microsoft Azure Cloud-Assets, die Serversysteme im Rechenzentrum der noris network AG sowie die Desktopsysteme, die nachrichtentechnischen Anlagen, die Netzwerke und die dazugehörige technische Infrastruktur an den oben aufgeführten Standorten. An der Durchführung der Dienstleistungsservices und des Betriebsmanagements beteiligt und somit im Anwendungsbereich des ISMS liegen die Organisationseinheiten Servicedesk, Betrieb und Projekt. Weiterhin wird die Steuerung der entsprechenden Dienstleister und besonders die Bereitstellung der Rechenzentrumskapazität der noris network AG mit einbezogen, um auch hier ein hohes Informationssicherheitsniveau aufrecht zu erhalten und zu verbessern.

Das eingeführte Managementsystem zur Informationssicherheit umfasst somit nicht die gesamte VINTIN Services GmbH. Schnittstellen zu den nicht betrachteten Organisationseinheiten bestehen in Form von Abhängigkeiten zu den Prozessen und dazugehörigen Systemen in den Organisationseinheiten Human Resources, Projekt und Entwicklung und der mit den anderen Tochterunternehmen der VINTIN Unternehmensgruppe gemeinsam genutzten Netzwerkinfrastruktur. Eine besondere Schnittstelle stellt MultiData dar. Die anderen Tochterunternehmen und Kunden haben darauf direkten oder eingeschränkten Zugang.

Informationssicherheitsziele

Die VINTIN verfolgt die folgenden langfristigen Informationssicherheitsziele durch den Betrieb des ISMS. Diese orientieren sich an dem Unternehmensleitbild, der Unternehmensstrategie und den Unternehmenszielen.

Kundenorientierung

Wir beraten bedarfsgerecht, tauschen uns intensiv mit unseren Ansprechpartnern aus, arbeiten auf Augenhöhe zusammen und schaffen so gemeinsam sichere IT-Lösungen mit maximalem Nutzen und dem größtmöglichen Maß an Sicherheit für unsere Kunden.

Verantwortung

Wir übernehmen in jeder Situation Verantwortung für unser Handeln. Dazu gehört auch, geltende Gesetze und Regelungen zu kennen und aus Überzeugung einzuhalten. Den gesetzlichen und vertraglichen Anforderungen an die Informationssicherheit ist in besonderen Maße nachzukommen, sodass das Risiko von Informationssicherheitsvorfällen und Schadenseinflüssen gemindert wird.

Vertrauen

Wir sind davon überzeugt, dass eine langfristige, erfolgreiche Zusammenarbeit zwischen Mitarbeitern, Lieferanten und Kunden nur auf einer soliden Vertrauensbasis möglich ist. Dies gilt auch für die Nichtweitergabe schützenswerter Daten an Dritte. Die Vertraulichkeit und Integrität aller Kunden- und Unternehmensdaten werden durch Maßnahmen zur Informationssicherheit und zum Datenschutz gewährleistet.

Teamwork

Komplexe IT-Projekte erfordern eine enge und koordinierte Zusammenarbeit über alle Fachbereiche hinweg. Durch eingespieltes Teamwork sind wir in der Lage, Außergewöhnliches zu leisten. Wir unterstützen unsere Kunden proaktiv und helfen ihnen durch unseren engagierten Einsatz anspruchsvolle Herausforderungen zu meistern. Dabei werden Erkenntnisse und Wissen zur Informationssicherheit geteilt und gemeinsam angewendet. Es wird bewusst auf die Informationssicherheit in der täglichen Arbeit geachtet.

Leistung

Wir entwickeln individuelle IT-Lösungen, die exakt zu den Anforderungen unserer Kunden passen und ihnen so echte Business-Mehrwerte liefern. Dem Anspruch einer hohen Verfügbarkeit der Kernprozesse, einschließlich zugehöriger Applikationen und unterstützender IT-Systeme sowie die Verfügbarkeit der Kundensysteme gemäß den vertraglichen Vereinbarungen und Regelungen werden wir gerecht. Ausfallzeiten sind zu minimieren.

Bewusstsein

Durch das Schaffen einer Sicherheitskultur im Unternehmen kann möglichen Schäden durch menschliches Fehlverhalten präventiv begegnet werden. Um unser Wissen auf dem neuesten Stand zu halten, investieren wir laufend in Sensibilisierung, Weiterbildung und Zertifizierungen. Bei der Planung und Ausübung aller relevanten Geschäftsprozesse werden stets technische und organisatorische Maßnahmen zur Verfügbarkeit, Integrität und Vertraulichkeit aller Daten und Information identifiziert und deren Umsetzung sichergestellt.

Informationssicherheitsmanagementorganisation

Die Geschäftsführung stellt den Chief Information Security Officer (CISO). Somit ist eine Entscheidungsrolle zur Informationssicherheit direkt in der obersten Ebene etabliert. Der CISO ist verantwortlich für die Informationssicherheit in der Organisation. Er ist für die Entwicklung und Einführung von Strategien zum Schutz und zur rechtmäßigen Nutzung von informationsverarbeitenden Anlagen verantwortlich und stellt sicher, dass Gesetzesvorgaben, Richtlinien und vertragliche Regelungen hinsichtlich Informationssicherheit eingehalten werden.

Weiterhin ist ein Information Security Manager beauftragt. Dieser ist direkt dem CISO unterstellt und initiiert und plant den Informationssicherheitsprozess und implementiert die entsprechende Organisation. Diese Informationssicherheitsmanagementorganisation (ISMO) besteht im Wesentlichen aus dem Information Security Manager, einer Information Security Assistance und einem IT-Risk Team.

Der Information Security Manager ist für alle Fragen rund um die Informationssicherheit in der Organisation zuständig. Er plant und koordiniert informationssicherheitsrelevante Maßnahmen und hat ein unmittelbares Vortragsrecht bei der Unternehmensleitung bezüglich des Status der Informationssicherheit sowie Informationssicherheitsvorfällen.

Die Information Security Assistance unterstützt den Information Security Manager beim Betrieb des ISMS (Planung, Organisation, Rekrutierung, Leitung, Überwachung, Betreuung und Motivation) sowie bei der Erstellung von Status- und Fortschrittreports, Kennzahlen und Präsentationen.

Hauptfunktion des IT-Risk-Managers sind die Anregung und Koordination von Tätigkeiten zur Identifikation, Bewertung und dem Umgang mit Informationssicherheitsrisiken in der gesamten Organisation.

Den Mitgliedern der ISMO werden von der Geschäftsführung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und ihre Aufgaben wahrnehmen zu können. Die ISMO wirkt auf die Einhaltung und Verbesserung sämtlicher Maßnahmen zur Informationssicherheit hin und erarbeitet Konzepte und Lösungsvorschläge für Geschäftsprozesse und Verfahren innerhalb des Geltungsbereiches.

Zentrale Aufgabe der ISMO ist der Betrieb und die Aufrechterhaltung des ISMS sowie die Kontrolle und Überprüfung der getroffenen Maßnahmen zur Informationssicherheit. Sofern personenbezogene Daten betroffen sind, ist der bestellte Datenschutzbeauftragte einzubinden.

Verbesserung der Informationssicherheit

Die Geschäftsleitung wird die ISMO und den Informationssicherheitsprozess aktiv unterstützen, überwachen und die ständige Verbesserung des Informationssicherheitsniveaus vorantrieben.

Die VINTIN Services GmbH wird sich am Standard DIN ISO/IEC 27001 orientieren. Dies schließt eine Realisierung der Managementelemente in Form von Dokumentenlenkung, interner Audits, Managementbewertung und der Anwendung des kontinuierlichen Verbesserungsprozesses (PDCA-Zyklus) mit ein.

Alle Mitarbeiter sowie die Geschäftsführung sind verpflichtet, allgemeine und arbeitsplatz-/bereichsspezifische Sicherheitsrichtlinien zu beachten und einzuhalten. Weiterhin sind alle Mitarbeiter angehalten, die Umsetzung und Aufrechterhaltung sämtlicher Maßnahmen aktiv zu erwirken und sich anbahnende und auftretende Informationssicherheitsvorfälle unverzüglich zu melden.

Erklärung

Diese Informationssicherheitsleitlinie tritt am 27.07.2017 in Kraft.

Die aktuelle und gültige Version der Leitlinie ist Version 1.6 vom 26.07.2018.