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

LEITLINIE FÜR DIE INFORMATIONSSICHERHEIT UND DEN DATENSCHUTZ DER VINTIN

30.09.2020

Informationssicherheits- und Datenschutzleitlinie als Bestandteil der organisationsweiten Sicherheitsstrategie und auf Grundlage der Anforderungen aus der Norm ISO/IEC 27001 und der EU DSGVO.

INHALTSVERZEICHNIS

Inhalt

DOKUMENTEN-INFORMATION

Dokumenten-Information

Titel:	LEITLINIE FÜR DIE INFORMATIONSSICHERHEIT UND DEN DATENSCHUTZ DER VINTIN
ERSTELLT DURCH:	Philipp Zacharias
VERSIONSNUMMER:	1.8
VERSIONSDATUM:	30.09.2020
FREIGEGEBEN VON:	Philipp Zacharias
FREIGABEDATUM:	30.09.2020

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
V1.7	25.06.2019	Philipp Zacharias	Aktualisierung	Final
V1.8.0	11.09.2020	Philipp Zacharias	Ergänzung Datenschutz	Entwurf
V1.8	30.09.2020	Patric Rudtke Philipp Zacharias	Finalisierung Datenschutz Freigabe	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 eine Niederlassung in Fulda.

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.

Ein weiterer Teil der Unternehmensgruppe ist die VINTIN Solutions GmbH. In enger Abstimmung mit den IT-Ansprechpartnern und -Verantwortlichen der Kunden realisiert sie neben aktiver Infrastruktur on Premise auch anspruchsvolle Lösungen in den Bereichen Cloud-Infrastruktur und managed Infrastruktur-Services.

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

Weiterhin stellt die Informationsverarbeitung eine entscheidende Rolle für die Wettbewerbsfähigkeit in der Informations- und Telekommunikationstechnikbranche 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 Unternehmensgruppe verabschiedet die Informationssicherheits- und Datenschutzleitlinie als Bestandteil der organisationsweiten Sicherheitsstrategie und auf Grundlage der Anforderungen aus der Norm ISO/IEC 27001 sowie der gesetzlichen Anforderungen der DSGVO.

Die Geschäftsführung sieht sich in der Pflicht, Maßnahmen zur Informationssicherheit und zum Datenschutz in den Geschäftsprozesse zu implementieren und deren Wirksamkeit im Rahmen eines Informationssicherheits- und Datenschutzmanagementsystems (IDMS) aufrecht zu erhalten und zu verbessern.

Grundsatz ist es, Informationssicherheit und Datenschutz in der gesamten Unternehmensgruppe aufrechtzuerhalten, zu verbessern und den Kunden einen entsprechenden Mehrwert zu bieten.

Geltungsbereich

Die Informationssicherheits- und Datenschutzleitlinie gilt für die VINTIN Services GmbH und VINTIN Solutions GmbH und den im IDMS festgelegten Anwendungsbereich sowie alle anderen Unternehmen der VINTIN Unternehmensgruppe.

IDMS-Anwendungsbereich

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

Anwendung findet das IDMS an den Standorten der VINTIN Services GmbH in Sennfeld und in Fulda und der VINTIN Solutions GmbH in Sennfeld. Die Räumlichkeiten in Fulda befinden sich in einer durch den Kunden bereitgestellten Lokation. Der Anwendungsbereich des IDMS 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, Amazon AWS-Dienste, die Serviceplattform der ENTIRETEC 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 IDMS liegen die Organisationseinheiten Servicedesk, Betrieb und Projektmanagement.

Weiterhin wird die Steuerung der entsprechenden Dienstleister und besonders die Bereitstellung der Rechenzentrumskapazität der noris network AG, der Serviceplattform der ENTIRETEC und der Verfügbarkeit der Services von AWS und Microsoft 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 und VINTIN Solutions GmbH. Schnittstellen zu den nicht betrachteten Bereichen bestehen in Form von Abhängigkeiten zu den Prozessen und dazugehörigen Systemen in den Organisationseinheiten Human Resources, Vertrieb, Projektdurchführung und Entwicklung und der mit den anderen Tochterunternehmen der VINTIN Unternehmensgruppe gemeinsam genutzten Infrastruktur.

Eine besondere Schnittstelle stellen die CRM- und Ticketsysteme MultiData und DokuSys dar. Die anderen Tochterunternehmen und Kunden haben darauf direkten oder eingeschränkten Zugang.

Informationssicherheits- und Datenschutzziele

Die VINTIN verfolgt die folgenden langfristigen Informationssicherheits- und Datenschutzziele durch den Betrieb des IDMS. 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 datenschutzkonforme und 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 und den Datenschutz ist in besonderem Maße nachzukommen, sodass das Risiko von Informationssicherheits- und Datenschutzvorfällen sowie 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 und Datenschutz geteilt und gemeinsam angewendet. Es wird bewusst auf die Informationssicherheit und den Datenschutz 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.

INFORMATIONSSICHERHEITS- UND DATENSCHUTZZIELE

Bewusstsein

Durch das Schaffen einer Sicherheitskultur und eines Datenschutzsbewusstseins 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 Einhaltung und Verbesserung von Datenschutz und Informationssicherheit identifiziert und deren Umsetzung sichergestellt.

Compliance

Über die Sensibilisierung und Schulung der Mitarbeiter hinaus wird die Einhaltung gesetzlicher, normativer und über Richtlinien und Arbeitsanweisungen gegebener Vorgaben mittels eines internen Kontrollsystems und den darin beschriebenen internen Audits nachgehalten.

Informationssicherheits- und Datenschutzmanagementorganisation

Die Geschäftsführung stellt einen für Informationssicherheit sowie einen für Datenschutz verantwortlichen Geschäftsführer. Somit sind Entscheidungsrollen zu Informationssicherheit und Datenschutz direkt in der obersten Ebene etabliert.

Die Informationssicherheits- und Datenschutzmanagementorganisation besteht aus dem Information Security Team und dem Datenschutzteam der VINTIN.

Das Information Security Team besteht aus Chief Information Security Officer (CISO), Information Security Assistance, IT-Risk Manager und IT-Risk Management Team.

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.

Er ist dem für Informationssicherheit verantwortlichen Geschäftsführer unterstellt und berät die Geschäftsführung hinsichtlich Themen der Informationssicherheit. Der CISO ist als Stabsstelle direkt unter der Geschäftsführung angesiedelt und in der gesamten Organisation weisungsbefugt hinsichtlich Informationssicherheitsthemen.

Außerdem plant und initiiert er den Informationssicherheitsprozess und implementiert die entsprechende Organisation. Der CISO ist für alle Themen und 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.

Der CISO leitet die Informationssicherheitsmanagementorganisation (Information Security Team).

Die Information Security Assistance ist dem CISO unterstellt und unterstützt den CISO beim Betrieb des IDMS (Planung, Organisation, Rekrutierung, Leitung, Überwachung und Betreuung) sowie bei der Erstellung von Status- und Fortschrittreports, Kennzahlen und Präsentationen.

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

Das Datenschutzteam setzt sich aus dem für die VINTIN-Gruppe bestellten Datenschutzbeauftragten, sowie den Mitarbeitern des Geschäftsfeldes Datenschutz zusammen.

Der Datenschutzbeauftragte ist durch das Unternehmen gemäß Artikel 37 DSGVO sowie § 38 BDSG (neu) bestellt. Er ist weisungsfrei in der Ausübung der Fachkunde und hat ein unmittelbares Vortragsrecht bei der Unternehmensleitung bezüglich der Konzeption des Datenschutzes im Unternehmen, bei Datenschutzvorfällen sowie Maßnahmen zur Verbesserung des Datenschutzes. Die Aufgaben des Datenschutzbeauftragten ergeben sich aus den Bestimmungen des Artikels 39 der DSGVO.

Die Mitglieder des Datenschutzteams unterstützen den DSB beim Betrieb des IDMS (Planung, Organisation, Rekrutierung, Leitung, Überwachung und Betreuung) hinsichtlich datenschutzrechtlicher Aspekte, sowie bei der Erstellung von Status- und Fortschrittreports, Kennzahlen und Präsentationen.

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

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

Verbesserung der Informationssicherheit und des Datenschutzes

Die Geschäftsleitung wird die IDMO und die Informationssicherheits- und Datenschutzprozesse aktiv unterstützen, überwachen und die ständige Verbesserung des Informationssicherheits- und Datenschutzniveaus vorantreiben.

Die VINTIN Services und VINTIN Solutions GmbHs werden 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 Informationssicherheits- und Datenschutzvorfälle unverzüglich zu melden.

Erklärung

Diese Informationssicherheits- und Datenschutzleitlinie tritt am 27.07.2017 in Kraft.

Die aktuelle und gültige Fassung der Leitlinie ist Version 1.8 vom 30.09.2020.