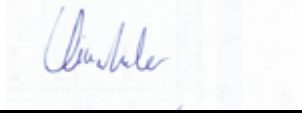
Zweck und Geltungsbereich:

Diese Richtlinie gilt für alle Mitarbeiter der Schönek Gruppe und all ihren Partnern. Die geltenden gesetzlichen Anforderungen sind in dieser Richtlinie berücksichtigt, werden einmal im Jahr auf ihre Gültigkeit überprüft, bei Änderungen angepasst und Mitarbeitern und externen Partnern (falls ein Projekt dies erfordert) zur Verfügung gestellt. Kundenspezifische Anforderungen zum Thema Informationssicherheit gelten ergänzend zu dieser Richtlinie, es sei denn, zwischen dem Kunden und der Firma Schönek wird eine andere Regelung vereinbart.
Die Erstellung dieser Richtlinie ist Teil der Implementierung des Informationsmanagementsystems nach VDA, wie im Managementreview des Geschäftsjahres 2021 festgelegt.

Dokumenteneigenschaft:

Verantwortung	Informationssicherheitsbeauftragte
Klassifizierung	Stufe 2 geringer Schutzbedarf
Gültigkeitszeit	Unbegrenzt
Überarbeitungsintervall	Jährlich
Geprüft im	Januar 2023
Nächste Überarbeitung	Dezember 2023

0	Neuerstellung
Revision	Beschreibung

Erstellt:	12.12.2022, Thiesbürger, Björn 
Geprüft	13.12.2022, Kinateder, Manuela 
Freigegeben:	13.12.2022, Freitag, Andreas 

Richtlinie zur Informationssicherheit

P12_RL04_00

Die Schönek Gruppe hat ein Managementsystem für Informationssicherheit (ISMS) etabliert. Nachfolgende Richtlinien sind damit verpflichtend:

1. Informationssicherheit stellt für die Schönek Gruppe ein äußerst wichtiges Qualitätsmerkmal der Datenverarbeitung dar, da alle wesentlichen strategischen und operativen Geschäftsprozesse im Unternehmen durch Informationstechnologie (IT) maßgeblich unterstützt werden.
   Ziel des Unternehmens ist es, die Daten und IT-Systeme in allen technikabhängigen und kaufmännischen Bereichen in ihrer Verfügbarkeit so zu sichern, dass die zu erwartenden Stillstandzeiten und der maximale Datenverlust toleriert werden können. Auch gilt es, die Integrität und Vertraulichkeit von sensiblen Unternehmensdaten und personenbezogenen Daten in ausreichender Weise zu garantieren; hierzu gehören Personaldaten ebenso wie technische Unterlagen. Schadensfälle mit hohen finanziellen Auswirkungen und immaterielle Folgen in Form von Imageschäden für das Unternehmen müssen verhindert werden. Beeinträchtigungen hinsichtlich der Verfügbarkeit der unternehmenseigenen Applikationen können ebenso gravierende Auswirkungen nach sich ziehen wie Unregelmäßigkeiten in Bezug auf die Integrität und Vertraulichkeit der verarbeiteten bzw. benutzten Informationen. Die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen, Anwendungen und IT-Systeme werden nicht nur durch Externe bedroht, sondern können auch durch interne Schwachstellen gefährdet werden.
   Ferner werden der Informationssicherheit im Hinblick auf Ausschreibungen Vorteile im Markt eingeräumt.

2. Die Geschäftsführung der Schönek Gruppe hat entschieden, dass ein angemessenes Sicherheitsniveau für einen normalen Schutzbedarf angestrebt werden soll. Grundlage für diese Entscheidung war eine kundenspezifische Anfrage zur Informationssicherheit und über die Werte der zu schützenden Güter sowie des vertretbaren Aufwands an Personal und Finanzmitteln.

3. Um Informationssicherheit gewährleisten zu können, sind angemessene technische und organisatorische Maßnahmen erforderlich. Diese können nur dann hinreichend wirksam sein, wenn alle Beschäftigten die möglichen Gefährdungen für die Informationssicherheit kennen und in ihren Aufgabenbereichen entsprechend verantwortlich handeln. Sensible Tätigkeiten sind durch die Schönek-Gruppe im Rahmen der Infrastrukturmatrix ermittelt und nach ihrer Bewertung klassifiziert. Regelmäßige Fortbildungen zur Informationssicherheit können hierbei unterstützen.

4. Die Maßnahmen für Informationssicherheit sollen auch dazu beitragen, dass die für das Unternehmen relevanten Gesetze, Vorschriften und vertragliche Verpflichtungen eingehalten werden.

5. Die Informationstechnik muss so betrieben werden, dass Geschäftsinformationen hinreichend schnell verfügbar sind. Ausfälle, die zu Terminüberschreitungen von mehr als einem Tag bei der Abwicklung von Aufträgen oder anderen wichtigen Geschäftsvorhaben führen, sind nicht tolerierbar. Informationssicherheit unterstützt damit auch eine funktionale Aufgabenerledigung.

6. Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, die Veränderung von Daten oder den Ausfall einer IT-Anwendung oder eines Systems entstehen. Informationssicherheit wirkt damit auch materiellen Schäden entgegen.

7. Vertraulichkeit und Integrität der für das Unternehmen wichtigen Informationen sind zu schützen, unabhängig davon, in welcher Form sie vorliegen. Auch im Umgang mit elektronischen Dokumenten und Informationen ist daher Geheimhaltungsanweisungen strikt Folge zu leisten.

8. Die Geschäftsführung ist das oberste Entscheidungsgremium. Sie verabschiedet auf Vorschlag der Informationssicherheitsbeauftragten diese Informationssicherheitsleitlinie.
   Die Geschäftsführung ist dafür verantwortlich, sicherzustellen, dass das ISMS entsprechend dieser Richtlinie umgesetzt und aktualisiert wird und dass die notwendigen Ressourcen verfügbar sind. Der IT-Leitung und dem Informationssicherheitsbeauftragten werden von der Geschäftsführung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden, zu informieren und die vom Management festgelegten Sicherheitsziele zu erreichen. Die Geschäftsleitung muss das ISMS mindestens einmal jährlich überprüfen (bzw. immer im Falle von erheblichen Änderungen) und freigeben. Zweck dieser Überprüfung durch das Management ist der Nachweis der Angemessenheit, Eignung und Wirksamkeit des ISMS. Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung (und damit die Informationssicherheit) verbleibt bei der Unternehmensleitung.

9. Die zentrale Instanz für die operative IT-Sicherheit ist die IT-Leitung. Sie ist für den sicheren Betrieb der IT und die Umsetzung geeigneter Sicherheitsmechanismen verantwortlich. In Zusammenarbeit mit dem Informationssicherheitsbeauftragten bringt sie die für die Informationssicherheit spezifischen Aspekte und Anliegen ein und ist für die Umsetzung geeigneter Sicherheitsmaßnahmen zuständig. Die IT-Leitung stellt sicher, dass der Informationssicherheitsbeauftragte frühzeitig in alle IT Projekte eingebunden wird.

10. Die Informationssicherheitsbeauftragte ist für die Koordination des Betriebs des ISMS verantwortlich sowie für die Berichterstattung über dessen Leistungsfähigkeit. Sie ist des Weiteren für die Koordination bzw. Umsetzung von Informationssicherheitstrainings und -programmen zur Bewusstseinsbildung (Awareness) für Mitarbeitende verantwortlich. Die Informationssicherheitsbeauftragte definiert, welche sich auf Informationssicherheit beziehenden Informationen durch wen und wann kommuniziert werden. Dies gilt sowohl für interne als auch externe Parteien. Sie ist für die Aufstellung und Implementierung des Plans für Training und Awareness verantwortlich, dem alle Personen unterliegen, die eine Rolle im ISMS innehaben.
    Die Einführung neuer Anwendungen, Verfahren, Prozesse und Infrastrukturkomponenten bedarf einer Freigabe durch den Informationssicherheitsbeauftragten. Dabei muss besonderes Augenmerk darauf gerichtet werden, dass durch den Einsatz der neuen Komponenten und Verfahren die Risiken hinsichtlich Informationssicherheit (Vertraulichkeit, Integrität,

Verfügbarkeit) nicht erhöht werden. Die Informationssicherheitsbeauftragte berät die Geschäftsführung und die Fachbereiche in Fragen der Informationssicherheit. Sie beobachtet laufend die technischen und organisatorischen Fortentwicklungen im Bereich der Informationssicherheit und schlägt in Abstimmung mit den betroffenen Unternehmensbereichen die notwendigen Maßnahmen vor. Des Weiteren ist sie frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase alle sicherheitsrelevanten Aspekte berücksichtigen zu können.

11. Die Mitarbeiter sollen sich stets der Bedeutung der Informationssicherheit bewusst sein und aktiv an der Abwehr und Bekämpfung von materiellen und ideellen Schäden mitwirken. Sie sollen verantwortungsbewusst mit den Informationssystemen und den darauf gespeicherten und dort verarbeiteten Daten umgehen und auf die Wahrung von Betriebs- und Geschäftsgeheimnissen achten. Der Schutz der Integrität, Verfügbarkeit und Vertraulichkeit von Werten unterliegt der Verantwortung der Eigentümer der jeweiligen Werte. Bei Unregelmäßigkeiten müssen die Mitarbeiter unverzüglich den Informationssicherheitsbeauftragten und ihre Vorgesetzten informieren. Es wird erwartet, dass jeder Nutzer von IT-Systemen die vorliegende Informationssicherheitsleitlinie kennt und beachtet.

12. Für alle Informationen, Geschäftsprozesse sowie die unterstützenden informationstechnischen Systeme und Infrastruktureinrichtungen werden Verantwortliche (Informations-, Prozess- und Systemeigentümer, Eigentümer von Zielobjekten) benannt. Diese sind dafür zuständig, die geschäftliche Bedeutung von Informationen und Technik einzuschätzen und darauf zu achten, dass die Mitarbeiter dieser Bedeutung entsprechend handeln. Sie verwalten Zugriffsrechte und Autorisierungen in ihrem Zuständigkeitsbereich und sind gegenüber der Leitung rechenschaftspflichtig. Sie sind auch dafür verantwortlich, externen Dienstleistern und Kooperationspartnern die Vorgaben der Schönek Gruppe zur Informationssicherheit zur Kenntnis zu geben und deren Einhaltung zu überwachen.

13. Beabsichtigte oder grob fahrlässige Handlungen, die Sicherheitsvorgaben verletzen, können finanzielle Verluste bedeuten, Mitarbeiter, Geschäftspartner und Kunden schädigen oder den Ruf des Unternehmens gefährden. Bewusste Verstöße gegen verpflichtende Sicherheitsregeln können arbeitsrechtliche und unter Umständen auch strafrechtliche Konsequenzen haben und zu Regressforderungen führen.

14. Diese Richtlinie zur Informationssicherheit bleibt bestehen, solange und soweit sie nicht durch eine spätere schriftliche Richtlinie aufgehoben oder verändert wird.

15. Prozessbeschreibungen und Arbeitsanweisungen, die sich auf diese Richtlinie beziehen gelten verpflichtend.

Nittenau im Dezember 2022
Schönek Gruppe

i. V. 

_____

Geschäftsleitung