Richtlinie zur Informationssicherheit

Februar 2024

Version 1/2024

Inhaltsverzeichnis

Vorwort des Vorstands 1
Grundlagen 2
1. Ziele der Informationssicherheit 2
1.1 Schutz von Informationswerten 2
1.2 Schutz von Kunden, Mitarbeitern und Reputation 2
1.3 Erfüllung rechtlicher Pflichten 2
2. Anwendungsbereich 2
2.1 Definitionen 3
2.2 Grundsätze der Informationssicherheit 4
3. Informationssicherheitsstrategie 5
4. Informationssicherheitsorganisation 6
4.1 Rollen und Verantwortlichkeiten 6

Richtlinie zur Informationssicherheit

Vorwort des Vorstands

Verantwortungsbewusste, nachhaltige Unternehmensführung und profitables Wachstum sind Leitbilder unseres unternehmerischen Handelns.

Wir sind davon überzeugt, dass ein Unternehmen seine Werte mit Hilfe der Informationssicherheit schützen muss, um nachhaltig erfolgreich sein zu können.

Die Bedrohungslage im Bereich Cyber- und Informationssicherheit steigt stetig an und mangelhafter Schutz vor diesen Bedrohungen kann ernsthafte Folgen für unser Unternehmen, unsere Kunden und Mitarbeiter haben.

Diese Richtlinie definiert das geltende Informations-Sicherheits-Management-System für die KAP AG und ihre Tochterunternehmen.

Sie gilt für alle Führungskräfte, Mitarbeiterinnen und Mitarbeiter des KAP-Konzerns und bildet einen wichtigen Baustein für eine erfolgreiche Zukunft.

Wir bitten alle Führungskräfte, Mitarbeiterinnen und Mitarbeiter des KAP-Konzerns darum, diese Richtlinie aufmerksam zu lesen und im Unternehmensalltag zu beachten.

KAP AG

Vorstand

Marten Julius Dr. Hartmut Sauer

Grundlagen

1. Ziele der Informationssicherheit

Ein Hauptziel der Informationssicherheit ist es, negative Auswirkungen auf KAP AG und ihre Tochterunternehmen (i.S.v. § 290 Abs. 1 HGB, „Tochterunternehmen“) im In- und Ausland (gemeinsam „KAP-Konzern“) auf ein akzeptables Risikoniveau zu reduzieren und ist somit Teil der firmenweiten Verantwortung für den Umgang mit Geschäftsrisiken.

1.1 Schutz von Informationswerten

Informationssicherheit soll Informationswerte vor dem Risiko des Verlusts, der Betriebsunterbrechung, des Missbrauchs, der unbefugten Weitergabe, der Unzugänglichkeit und der Beschädigung schützen.

1.2 Schutz von Kunden, Mitarbeitern und Reputation

Mangelhafter Schutz von Informationen und Dienstleistungen vor Cyber- und Informationssicherheit Bedrohungen können ernste Folgen für unsere Kunden und Mitarbeiter haben.

Die Reputation, Marke und Finanzstabilität können gleichwohl Schaden nehmen.

Das Informations-Sicherheits-Management-System (das „ISMS“) der KAP AG („KAP“) soll das Vertrauen unserer Kunden, Lieferanten und sonstigen Geschäftspartner, der Aktionäre, der Mitarbeiter und der allgemeinen Öffentlichkeit in die Integrität und Zuverlässigkeit des KAP-Konzerns und seiner Produkte schützen.

Damit trägt es dazu bei, die Reputation des KAP-Konzerns und seiner Mitarbeiter zu erhalten und zu stärken.

1.3 Erfüllung rechtlicher Pflichten

Die Unternehmen des KAP-Konzerns sind weltweit aktiv. Zahlreiche Gesetze regeln länderübergreifend die Cyber- und Informationssicherheit sowie den Datenschutz.

Bei entsprechender Gefährdungslage besteht in einigen Ländern eine rechtliche Meldepflicht für Datenschutzvorfälle / Cyberangriffe. Diesen Anforderungen soll das ISMS ebenfalls genügen.

2. Anwendungsbereich

Diese Richtlinie zur Informationssicherheit („Richtlinie“) der KAP regelt das ISMS des KAP-Konzerns.

Sie gilt für alle Führungskräfte, Mitarbeiterinnen, Mitarbeiter und vorübergehend Beschäftigten des KAP-Konzerns sowie für externe Dienstleister, die konzernintern eingesetzt sind („Mitarbeiter[1]“).

[1] Im Folgenden wird aus Gründen der Lesbarkeit auf die gleichzeitige Verwendung der männlichen, weiblichen und diversen (m/w/d) Sprachform verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Das ISMS dient dem Management der rechtlichen und regulatorischen Risiken, die vom Code of Conduct des KAP-Konzerns und anderen, diesen ergänzenden Richtlinien erfasst sind.

Insbesondere dient diese Richtlinie dazu,

- die Grundlagen des ISMS festzulegen und so den Mitarbeitern Orientierung und Hilfestellung zu bieten;
- die Strukturen und Berichtswege innerhalb der Informationssicherheits-Organisation des KAP-Konzerns darzustellen und die Schnittstellen zu anderen Fachbereichen zu bestimmen und
- die Anforderungen an das aktive Management von Informationssicherheits-Risiken und die zugehörigen Prozesse zu beschreiben.

Die Richtlinie wird ergänzt mit der Richtlinie für Fachliche & Technische Anforderungen zur Informationssicherheit, der Sicherheitsrichtlinie für Vorgesetzte und Mitarbeitende, sowie der Datenschutzrichtlinie (Code of Conduct für den Datenschutz).

Wo strengere lokale Gesetze und Vorschriften gelten, als in dieser Richtlinie aufgeführt, müssen diese Vorgaben im betreffenden Rechtsgebiet eingehalten werden.

2.1 Definitionen

Informationen und Daten : Informationen stehen für den Inhalt / die Bedeutung von Daten. Als Daten beschreibt man die Darstellung von Informationen in elektronischer Form oder anderweitigen Formen (zum Beispiel gespeichert auf einer Festplatte, auf Papier ausgedruckt, auf eine CD gebrannt, auf USB kopiert, als Audio gespeicherte/archivierte Gespräche, Video)

Informationssicherheit : Definiert als Methode zum Schutz von Informationen und Informationssystemen vor unbefugtem Zugriff beziehungsweise missbräuchlicher Verwendung, Offenlegung, Unterbrechung und Änderung sowie vor Datenverlust oder Vernichtung. Sie wird in der Regel durch organisatorische und technische Maßnahmen unterstützt.
Informationssicherheit steht im Zusammenhang mit dem Datenschutz und dem Ziel des Schutzes der **Verfügbarkeit, Vertraulichkeit, Integrität** und **Authentizität** von Informationen.

Informationswert : Ein Informationswert sind Informationen, die in beliebiger Weise verwahrt werden und für die KAP wertvoll sind. Bei den Informationen könnte es sich um Kunden-, Mitarbeiter- oder Unternehmensinformationen handeln, die in jeglicher Form innerhalb oder außerhalb der KAP Räumlichkeiten übertragen, verarbeitet oder gespeichert werden können.
Darunter u.a. mündlich, schriftlich, auf Papier oder elektronisch, sowie strukturierte Daten in einer Datenbank, einer Anwendung oder anderer Form. Unstrukturiert auf einer gemeinsam genutzten Festplatte, einem Laufwerk, einer SharePoint-Site o.ä.

Datenschutz : Definiert als das Recht eines Betroffenen, zu entscheiden und zu bestimmen, wer zu welchem Zeitpunkt aus welchem Grund befugt ist, auf seine personenbezogenen Daten zuzugreifen und unter welchen Bedingungen seine personenbezogenen Daten verwendet und an Dritte weitergegeben werden dürfen.

Datenschutz befasst sich mit einer Teilmenge aller Informationen und Daten eines Unternehmens. Es bezieht sich ausschließlich nur auf personenbezogene Daten, steht jedoch insoweit im Zusammenhang zur Informationssicherheit.
(Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare lebende Person beziehen. Verschiedene Teilinformationen, die gemeinsam zur Identifizierung einer bestimmten Person führen können, stellen ebenfalls personenbezogene Daten dar.)

2.2 Grundsätze der Informationssicherheit

Die Informationssicherheit basiert auf den folgenden Grundsätzen :

Eigentümerschaft von Informationen - Sämtliche Informationsbestände müssen einem Eigentümer zugewiesen werden, der für den Gebrauch innerhalb eines Unternehmens verantwortlich ist. In diesem Zusammenhang ist mit „Verantwortlichkeit“ die Verantwortung gemeint, die zum Schutz von Informationsbeständen erforderlichen Sicherheitsmaßnahmen zu bestimmen und aufrechtzuerhalten. Dies erfolgt durch die Klassifizierung.

Klassifizierung von Informationswerten – Alle Informationswerte müssen klassifiziert und entsprechend ihren Anforderungen an die Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität behandelt werden. Dabei sind Geschäftsanforderungen sowie die geltenden rechtlichen, vertraglichen oder regulatorischen Vorschriften und Einschränkungen zu beachten. Zur Erleichterung der Durchführung kontinuierlicher und effektiver Informationssicherheitsmaßnahmen muss das Basismodell für die Klassifizierung von Informationswerten der KAP gemäß der Guideline zur Klassifizierung und Handhabung von Informationen herangezogen werden.

Schutz von Informationswerten – Geeignete Informationssicherheitsmaßnahmen müssen die Geschäftsanforderungen, eine Risikobeurteilung, wirtschaftliche Effizienz, rechtliche, vertragliche oder regulatorische Vorschriften und Beschränkungen sowie verfügbare technische und versicherungsbezogene Vorkehrungen berücksichtigen. Da Informationen und Systeme nicht hundertprozentig geschützt werden können, müssen die Restrisiken (das Risikoniveau nach der Umsetzung von Gegenmaßnahmen) beurteilt, dokumentiert und bearbeitet werden.

Informationssicherheitskontrollen – Bei der Einführung von Informationssicherheitskontrollen ist ein ganzheitlicher Ansatz erforderlich. Solche Kontrollen sollen nicht isoliert betrachtet oder umgesetzt werden. Beispielsweise müssen, wann immer es schwierig ist, eine bestimmte Maßnahme umzusetzen, entsprechende kompensierende Kontrollen eingeführt werden.

Protokollierung und Überwachung auf Systemebene – Es müssen Methoden zur Erkennung und Protokollierung von Sicherheitsverletzungen, Anomalien, Vorfällen und unbefugten Handlungen eingeführt sein. Systeme sollten überwacht und Informationssicherheitsvorfälle aufgezeichnet werden. Es sollten Benutzer- und Fehlerprotokolle geführt werden, um zu gewährleisten, dass Informationssystemprobleme erkannt werden.

Vorfallmanagement und Sicherheitsverletzungen – Es sind Prozesse zur Meldung von Vorfällen und für ein vernünftiges und effizientes Handeln erforderlich, die Geschäftsunterbrechungen begrenzen oder vermeiden und die Lehren aus Vorfällen ziehen, um das Risiko des Schadenseintritts in Zukunft zu minimieren und Schutzmaßnahmen zu verbessern. Es liegt in der Verantwortung aller Mitarbeiter, Verletzungen, Schwächen und Störungen zu melden.

Need-to-Know Prinzip – Das Need-to-Know Prinzip besagt, dass ein Benutzer nur Zugang zu den Informationen haben darf, die seine berufliche Funktion gerade eben erfordert. Der Zugang zu Informationswerten muss ausdrücklich genehmigt werden. Standardmäßig besteht kein Zugriff.

Aufgabenteilung / Vier-Augen-Prinzip – Wertvolle Informationen und hochriskante Prozesse dürfen nie ausschließlich von einer Person kontrolliert werden. Die Aufgabenteilung und das Vier-Augen-Prinzip sollten angewandt werden, um gegensätzlichen Fähigkeiten zu trennen oder Integritätsschwächen zu erkennen beziehungsweise um Betrug beim Umgang mit Informationen vorzubeugen.

Schutz vor Datenlecks (Data Leakage Prevention DLP) – Möglichkeiten für Datenlecks müssen begrenzt werden. Die Eigentümer von Daten müssen die Vorgaben für den Schutz festlegen. Mögliche Maßnahmen sind Beschränkung von Massendrucks (email), Downloadfunktionen am Arbeitsplatz und Kopieren auf externe Medien, Anonymisieren und Maskieren von Daten usw.

Zutrittskontrollen - Zutrittskontrollmaßnahmen sollen Unbefugten den physischen Zutritt zu Datenverarbeitungsanlagen, mit denen Informationen und personenbezogene Daten verarbeitet oder genutzt werden, verwehren.

Zugangskontrollen - Zugangskontrollmaßnahmen sollen verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Zur Umsetzung dieser Kontrollmaßnahme ist ein Passwortmanagement nötig; u.a. Zwei-Faktor-Authentifikation, Passwortrichtlinien sowie eine entsprechende Protokollierung der Passwortnutzung von privilegierten Accounts.

3. Informationssicherheitsstrategie

Die vorliegende Richtlinie definiert die Rahmenbedingungen für das Management der Informationssicherheit. Wir streben ein angemessenes Sicherheitsniveau an und richten uns an internationalen Normen, wie der ISO27001, der europäischen NIS2-Richtlinie und dem nationalen Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aus.

Mit Verabschiedung dieser Richtlinie legt der Vorstand der KAP somit den Grundstein für die Einführung des ISMS. Unterstützt durch eine Software werden im ISMS standardisierte Verfahren, Richtlinien und vorgegebene Maßnahmen festgelegt, um Unternehmenswerte zu schützen und Risiken zu minimieren.

Als zentrale Instanz ernennt der Vorstand der KAP einen Informationssicherheitsbeauftragten, der die Themenverantwortlichkeit der Informationssicherheit übernimmt.

Er berichtet in seiner Funktion an die Geschäftsführung. In enger Zusammenarbeit mit der Informationssicherheitsorganisation werden notwendige Maßnahmen geplant und realisiert.

Dem Informationssicherheitsbeauftragten werden alle erforderlichen Ressourcen zur Ausübung seiner Funktion bereitgestellt. Ihm werden geeignete Qualifizierungsmöglichkeiten ermöglicht, um auf aktuelle sicherheitsrelevante Themen reagieren zu können.

Zum Erhalt, sowie zur kontinuierlichen Verbesserung der Informationssicherheit, wird in regelmäßigen Abständen geprüft, ob ausgewählte Sicherheitsmaßnahmen ausreichenden Schutz bieten.

Meldungen über Sicherheitsvorfälle werden von der Informationssicherheitsorganisation analysiert, dokumentiert und behandelt. Entsprechende Melde- und Berichtswege müssen etabliert werden.

Unerlässlich dabei ist das Anzeigen von Sicherheitsrisiken und Vorfällen durch die Mitarbeiter des KAP-Konzerns.

4. Informationssicherheitsorganisation

Der Vorstand bzw. die Geschäftsführung trägt die Gesamtverantwortung für die Informationssicherheit im jeweiligen Unternehmen. Der Vorstand bzw. die Geschäftsführung kann Aufgaben zum Informationssicherheitsmanagement an Verantwortliche delegieren. Die Gesamtverantwortung verbleibt dennoch immer beim Vorstand bzw. bei der Geschäftsführung.

Um den Sicherheitsprozess zu planen, umzusetzen sowie aufrechtzuerhalten, wird eine Informationssicherheitsorganisation gebildet.

Diese besteht aus nachfolgenden Verantwortlichkeiten:

- Informationssicherheitsbeauftragter
- Director IT / KAP
- IT Security Team
- Datenschutzbeauftragter
- IT Leitung Tochterunternehmen / Beauftragte der Segmente

Die Organisation ist in entsprechenden Themengebieten durch Verantwortliche der Leitungsebene zu unterstützen. Es ist regelmäßig zu überprüfen, ob die aufgebaute Organisation noch für ihren Zweck angemessen ist, oder neuen Rahmenbedingungen angepasst werden muss.

4.1 Rollen und Verantwortlichkeiten

Informationssicherheitsbeauftragter („ISB“)

- Überwachung und Bewertung der Informationssicherheitsrichtlinien und -verfahren des KAP-Konzerns
- Identifizierung von Risiken und Bedrohungen für die Informationssicherheit und Entwicklung von Maßnahmen zur Minimierung dieser Risiken
- Schulung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für Informationssicherheitsfragen
- Koordination von Sicherheitsprüfungen und Audits sowie Zusammenarbeit mit internen und externen Prüfern
- Reaktion auf Sicherheitsvorfälle und Untersuchung von Sicherheitsverletzungen
- Sicherstellung der Einhaltung gesetzlicher und regulatorischer Anforderungen im Bereich der Informationssicherheit

Director IT / KAP

- Verantwortlich für die IT-Abteilung der KAP

- Strategische Führung der IT-Infrastruktur des gesamten Konzerns in Zusammenarbeit mit der IT Leitung der Tochterunternehmen / Beauftragte der Segmente
- Operative und strategische Führung der IT-Infrastruktur des gesamten Konzerns
- Planen und Sicherstellen eines effizienten, sicheren und verlässlichen IT-Betriebs
- Entwicklung und Realisierung einer IT-Strategie
- Als oberster IT-Verantwortlicher des KAP-Konzerns obliegt ihm die Planung, der Betrieb und die Weiterentwicklung der IT-Systeme und Prozesse innerhalb der Organisation

IT Security Team

- Das IT Security Team nimmt die Aufgabengebiete "Detektion", "Reaktion" und "Prävention" sowie andere damit verbundene Tätigkeiten wahr
- Ziel des Aufgabengebiets "Detektion" ist dabei, sicherheitsrelevante Ereignisse zeitnah und zuverlässig zu erkennen
- Falls notwendig, ergreift das Team im Rahmen des Aufgabengebietes "Reaktion" geeignete Maßnahmen
- Erkenntnisse über Cyber-Gefahren, insbesondere über Bedrohungen, Schwachstellen und Vorfälle, werden im Aufgabengebiet "Prävention" erfasst, analysiert und aufbereitet

Datenschutzbeauftragter

- Er überprüft, ob die personenbezogenen Daten im KAP-Konzern ausreichend geschützt werden und ob die DSGVO Richtlinien korrekt umgesetzt werden
- Muss eine Datenschutz-Folgenabschätzung durchgeführt werden, berät der Datenschutzbeauftragte den Verantwortlichen dabei
- Der Datenschutzbeauftragte bildet die Schnittstelle zwischen KAP-Konzern und Aufsichtsbehörde. Er arbeitet mit beiden Seiten zusammen und ist die Anlaufstelle bei konkreten Fragen
- Eine weitere Aufgabe ist die Schulung und regelmäßige Sensibilisierung der Mitarbeiter zum Thema Datenschutz im KAP-Konzern

IT Leitung Tochterunternehmen / Beauftragte der Segmente

- Verantwortlich für die lokale IT-Abteilung, IT-Applikationen und IT-Infrastruktur
- Dokumentieren und überwachen der lokalen IT-Assets
- Die lokale IT Leitung trägt die Verantwortung für alle lokalen IT-Risiken
- Planen und Sicherstellen eines effizienten, sicheren und verlässlichen lokalen IT-Betriebs
- Lokale Umsetzung der konzernweiten IT-Strategie und der Informationssicherheits-Strategie

Die Verantwortung für die Informationssicherheit liegt jedoch nicht allein bei der Informationssicherheitsorganisation, der IT-Abteilung oder den Führungskräften.

Jeder Mitarbeitende trägt Verantwortung für die Sicherheit von Informationen und Systemen der Organisation.