Anforderungen zur Informationssicherheit für Mitarbeiter und Vorgesetzte

Februar 2024

Version 1/2024

Inhaltsverzeichnis

Grundlagen

1. Anwendungsbereich

Diese Richtlinie der KAP AG („KAP“) regelt Anforderungen zur Informationssicherheit für Mitarbeiter und Vorgesetzte, als ein Bestandteil des Informations-Sicherheits-Management-System (das „ISMS“) von KAP und ihren Tochterunternehmen (i.S.v. § 290 Abs. 1 HGB, „Tochterunternehmen“) im In- und Ausland (gemeinsam „KAP-Konzern“).

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

Die Richtlinie ist eine Ergänzung zur Informationssicherheitsrichtlinie und der Richtlinie für Fachliche & Technische Anforderungen zur Informationssicherheit, sowie der Datenschutzrichtlinie (Code of Conduct für den Datenschutz).

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

Informationen beziehen sich auf den Inhalt oder die Bedeutung von Daten und können auf jede Art und Weise aufbewahrt werden (physische Kopie, E-Mail, Datei auf dem Rechner usw.) Wie in der Informationssicherheitsrichtlinie definiert, steht die Informationssicherheit im Zusammenhang mit dem Datenschutz und dem Ziel des Schutzes der

Verfügbarkeit, Vertraulichkeit, Integrität und **Authentizität** von Informationen.

Cybersicherheit ist der Prozess des Schutzes von Informationen gegen digitale Bedrohungen. Maßnahmen der Cyber- und Informationssicherheit erstecken sich über den gesamten Lebenszyklus von Informationen.

Verhaltenskodex der KAP

Schutz vertraulicher Informationen

Der KAP-Konzern stellt sicher, dass schützenswerte Daten (Geschäftsgeheimnisse und personenbezogene Daten) sachgerecht und gesetzeskonform erhoben, verarbeitet, gesichert und gelöscht werden. Er verpflichtet seine Beschäftigten entsprechend. Schützenswerte Daten dürfen nicht unbefugt an Dritte weitergegeben oder in anderer Form veröffentlicht werden und sind dahingehend zu schützen.

Der KAP-Konzern schützt Unternehmensdaten ebenso wie personenbezogene Kunden- und Mitarbeiterdaten mit allen dem Konzern zur Verfügung stehenden geeigneten und angemessenen technischen und organisatorischen Mitteln vor unberechtigtem Zugriff, unbefugter beziehungsweise missbräuchlicher Verwendung, Verlust und vorzeitiger Vernichtung. Alle Mitarbeitenden sind daher verpflichtet, erforderliche Maßnahmen zu treffen, um die Sicherheit von IT-Systemen in Bezug auf internen und externen Missbrauch und Bedrohungen zu gewährleisten. Zudem achtet das Unternehmen bei der Erhebung, Speicherung, Verarbeitung und Übertragung personenbezogener Daten von Mitarbeitenden, Kunden oder anderen Dritten auf größte Sorgfalt und strenge Vertraulichkeit sowie die Einhaltung geltender Gesetze und Regeln.

---

[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.

2. Anforderungen zur Informationssicherheit an Mitarbeiter

Zum Schutz unserer Kunden, Partner und Kollegen sind wir gemeinsam gefordert, Informationen vor Cyber- und Informationssicherheitsrisiken zu schützen.

Dieses Dokument soll verdeutlichen, warum jeder Einzelne wichtig ist, Informationen zu schützen. Es definiert die Anforderungen für Mitarbeiter und Vorgesetzte und gibt nützliche Hinweise, diese im Arbeitsalltag anzuwenden.

2.1 Passwörter, Zugangsdaten und Zutrittskarten

Ihre Zugangsdaten einschließlich Passwörter, PINs, Token und Zutrittskarten sind persönliche Daten, die ausschließlich von Ihnen verwendet werden dürfen. Geben Sie ihre Zugangsdaten niemals weiter, da sie nur Ihnen den Zugang zu Systemen und Einrichtungen erlauben und mit ihrer persönlichen Unterschrift gleichzusetzen sind.

Sie sind verantwortlich für jede Aktion, die mit ihren Zugangsdaten durchgeführt werden. Ihre Zugangsdaten einschließlich Passwörter, PINs, Token oder Zutrittskarten;

- dürfen an niemanden weitergeben werden, unabhängig von Rang oder Rolle.
- müssen vor Diebstahl oder Missbrauch geschützt werden. Ein Verlust oder potenzieller Missbrauch muss unverzüglich ihrem Vorgesetzten und der Informationssicherheitsorganisation gemeldet werden.
- dürfen nur für genehmigte Zwecke verwendet werden.

2.2 Physische Sicherheit

Die Informationssicherheit geht über den digitalen Bereich hinaus und umfasst auch den Schutz von Informationen in physischer Form.

Sie haben individuelle Verantwortung für ihre Zutrittskarte/-Chip und dürfen diese auch niemals an andere weitergeben.
Zugang durch kontrollierte Türen und Zugangsschranken dürfen nur berechtigten Personen gewährt werden.

Ihre Besucher müssen sich anmelden und dürfen nur in Begleitung und unter Beaufsichtigung in ein Gebäude oder einen Bereich eigelassen werden. Verdächtige Personen oder Aktivitäten müssen umgehend den verantwortlichen Personen für die physische Sicherheit gemeldet werden.
Um physische Dokumente zu sichern, müssen Sie die „Clear Desk“ Regeln für einen sicheren Arbeitsplatz beachten. Dies gilt für ihren eigenen Arbeitsbereich im Büro, im Homeoffice, sowie gemeinsam genutzte Bereiche.

- Sperren Sie Ihren Bildschirm mit einem (Passwort-) geschützten Bildschirmschoner, auch wenn Sie den Arbeitsplatz nur kurz verlassen.
- Lassen Sie „vertrauliche“ oder „streng vertrauliche“ Dokumente niemals unbeaufsichtigt am Arbeitsplatz oder im Drucker liegen.
- Schließen Sie Fenster und Türen, wenn das Büro nicht besetzt ist.
- Tragen Sie mobile Geräte bei sich oder schließen Sie sie weg.
- Entsorgen Sie Daten und Informationen sicher, z B. einen USB-Stick mit Unternehmensdaten in einer Datentonne, das Protokoll einer internen Sitzung im Schredder.

- Beachten Sie auch bei der Nutzung von Besprechungsräumen sowie von zentralen Kopierern, Druckern und Faxgeräten die Sicherheitsregeln und lassen Sie keine internen Unterlagen liegen.

2.3 Informationssicherheit

Informationen beziehen sich auf den Inhalt oder die Bedeutung von Daten und können in beliebiger Form aufbewahrt werden; z.B. E-Mail, Datei auf dem Desktop, physische Kopie usw.

Wie in der Informationssicherheitsrichtlinie definiert, ist Informationssicherheit der Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen.

Alle Informationen, unabhängig von ihrer Form, müssen auf der Grundlage der Ihnen zugewiesenen Klassifizierung geschützt werden. Dies gilt während des kompletten Lebenszyklus.

Dieser Informationslebenszyklus beinhaltet :

a) Erstellung
b) Handhabung und Transport
c) Speicherung und Archivierung
d) Vernichtung und Entsorgung

Sie, als Informationseigentümer, tragen die Verantwortung, dass die von Ihnen erstellten Informationen nach ihrer Vertraulichkeit klassifiziert werden. Maßgeblich hierfür ist die Richtlinie Klassifizierung & Handhabung von Informationen.

- Wenn Sie neue Informationen erstellen oder bestehende wesentlich verändern, müssen Sie die Vertraulichkeitsqualifizierung erneut bestimmen
- Für Informationen gilt immer das vom Informationseigentümer verlangte Schutzniveau
- Die Standardklassifizierung für Informationen ist „intern“
- Informationen die als „vertraulich“ oder darüber klassifiziert werden, müssen mit der entsprechenden Klassifizierung gekennzeichnet werden

2.4 Sichere Kommunikation

Das Internet, E-Mails, Messaging Services und virtuelle Konferenzen sind zunehmend unverzichtbare Hilfsmittel im täglichen Berufs- und Privatleben.

Leider bilden diese auch ein nicht zu unterschätzendes Einfallstor für Cyberangriffe. Kleine Fehler oder mangelnde Aufmerksamkeit für Details können hier große Folgen haben.

Für Ihre geschäftliche Kommunikation dürfen ausschließlich die vom Unternehmen zur Verfügung gestellten Systeme und genehmigte Kommunikationskanäle verwendet werden.

Sie müssen sicherstellen, dass die Verteilung von Informationen über genehmigte Kanäle angemessen ist und immer nach dem „Need to Know“ Prinzip überprüft und gehandelt wird.

Das „Need to Know“ Prinzip ist die Anforderung, Zugriffsrechte auf Informationen und Systeme auf das zu beschränken, was für eine Person erforderlich ist, um ihre Aufgaben zu erfüllen.

- Bei der Verteilung von Informationen die nicht als „öffentlich“ eingestuft sind, müssen Anstrengungen unternommen werden um sicherzustellen, dass alle Empfänger und Teilnehmer authentifiziert werden, bevor die Weitergabe / Verteilung beginnt.

- Informationen, die auf einem gemeinsamen Speichersystem mit Zugangskontrollen geschützt sind, dürfen nur an befugte Personen weitergegeben werden („Need to Know“)
- Es dürfen nur autorisierte Online-Speicher Systeme / File Share Dienste verwendet werden.
- Externe Speichermedien / Wechseldatenträger dürfen nur in Ausnahmefällen verwendet werden, dazu gehören u.a. USB-Sticks, externe Festplatten, CDs, DVDs. Diese müssen zwingend vor der Nutzung auf Viren oder sonstige Malware untersucht werden.
- Informationen, die mit Hilfe von solchen Medien verbreitet werden, müssen verschlüsselt sein, potenzielle Verluste müssen gemeldet werden.
- Sprachgesteuerte Smart Devices ermöglichen, Geräte mittels Spracherkennung zu aktivieren. Dies kann sehr praktisch sein. Damit ihre geschäftlichen Gespräche auch zuhause sicher bleiben, empfiehlt es sich allerdings, diese Dienste zu deaktivieren.
- Verwenden Sie ihre geschäftliche E-Mail Adresse ausschließlich für geschäftliche Zwecke und geben Sie keine Details über das Unternehmen, ihre Rolle, ihre Kollegen o.ä. in sogenannten Social Media Kanälen preis.

2.5 Schützen Sie ihren Arbeitsplatz und ihre Geräte

Der tägliche Einsatz von elektronischen Geräten ist heutzutage selbstverständlich und sie sind ein sehr wichtiges Mittel geworden, um auf Informationen zuzugreifen und unsere Aufgaben zu erledigen.

Diese Geräte und auch das Internet sind aber gleichwohl auch Einfallstore für Angriffe durch Kriminelle. Eine ordnungsgemäße Nutzung der bereitgestellten Geräte und der Software sind von großer Bedeutung für den Schutz von Informationen.

- Nur bereitgestellte bzw. autorisierte Hard- und Software dürfen genutzt werden, um auf Unternehmensdaten zuzugreifen, sie zu verarbeiten oder zu speichern.
- Sie dürfen keine technischen oder organisatorischen Sicherheitsfunktionen umgehen, verändern oder aushebeln.
- Ungewöhnliche Änderungen an der Ausstattung ihres Arbeitsplatzes wie z.B. ausgetauschte Systeme, zusätzliche Hardware, manipulierte Software oder verschwundene Peripheriegeräte müssen Sie unbedingt hinterfragen und melden.
- Sie müssen verlorene oder gestohlene Geräte unverzüglich melden.
- Wenn Sie das Unternehmen verlassen, müssen Sie alle elektronischen Geräte zurückgeben.

2.6 Social Engineering, Phishing & Schadsoftware

Als Mitarbeiter können Sie leicht zur Zielscheibe von Kriminellen werden, die sich Zugang zu Informationen und Systemen des Unternehmens verschaffen wollen.

Beim Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um Personen zu manipulieren. Kriminelle verleiten das Opfer auf diese Weise z.B. dazu, Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware auf dem privaten Gerät oder einem Computer im Firmennetzwerk zu installieren.

Phishing ist eine Form des Social Engineering, bei der betrügerische E-Mails, Textnachrichten, Telefonanrufe oder Websites darauf abzielen, das Opfer zu verleiten, Links zu klicken,

gefälschte Websites zu besuchen, Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware zu installieren.

- Sie sollten sich der Risiken durch Cyber-Bedrohungen, Schadsoftware und Social Engineering bewusst sein und Maßnahmen ergreifen, um diese Risiken zu minimieren.
- Zur Verfügung gestellte Schulungsmaterialen und Guidelines zum Thema Informationssicherheit und Cybersicherheit sind unbedingt zeitnah durchzuarbeiten und zu beachten.
- Erlauben Sie niemals einem Unbefugten den Fernzugriff oder die Fernsteuerung ihres Gerätes. Falls Sie dies doch getan haben, melden Sie dies sofort an die IT Abteilung.
- Melden Sie ungewöhnliche Aktivitäten an ihren elektronischen Geräten, genauso wie auffällige Informationsanfragen von fremden Personen, welche Sie abweisen.
- Phishing E-Mails können z.B. im Outlook über einen Button „Spam an IT melden“ weitergeleitet werden.

3. Verantwortung von Vorgesetzten

Vorgesetzte tragen im Rahmen ihrer Aufsichts- und Fürsorgepflichten zusätzliche Aufgaben im Bereich der Informationssicherheit gegenüber ihren Mitarbeitern und dem jeweiligen Unternehmen im KAP-Konzern.

Sie müssen wichtige Nachrichten aus diesem Bereich an ihre Mitarbeiter weitergeben und Sie sind Empfänger von deren Meldungen über Auffälligkeiten und Aktivitäten, welche die Informationssicherheit beeinträchtigen können.

Zusätzlich überwachen Sie auch die Zugriffsrechte auf Informationen und Systeme ihrer Mitarbeiter, dies gilt besonders bei Ein- oder Austritten und Änderungen. Sie sind verantwortlich für die Umsetzung und Kontrolle des „Need to Know“ Prinzip in ihrem Bereich.

Der wichtigste Aspekt jedoch ihrer zusätzlichen Aufgaben ist die Verpflichtung zur Förderung einer angemessenen und pro-aktiven Informationssicherheitskultur bei ihren Mitarbeitern. Die Informationssicherheitskultur ist ein Bestandteil der Unternehmenskultur und bestimmt die Wahrnehmung, das Denken, Fühlen und Handeln in Bezug auf die Informationssicherheit.

- Überprüfen Sie die Zugriffsrechte und Zugangsberechtigungen ihrer Mitarbeiter in regelmäßigen Abständen
- Handeln Sie bei der Genehmigung von neuen Berechtigungen immer nach dem „Need to Know“ und „Least-Privilege“ Prinzip
- Sie müssen dafür sorgen, dass die Personalabteilung rechtzeitig informiert wird, damit Wechsel und Austrittsereignisse, ihre Mitarbeiter betreffend, zeitnah umgesetzt werden können.
- Sie müssen die Rückgabe von elektronischen Geräten und Zutrittskarten ihrer Mitarbeiter sicherstellen, wenn diese das Unternehmen verlassen.

4. Inkrafttreten

Diese Richtlinie tritt mit ihrer Verabschiedung durch den Vorstand der KAP AG in Kraft.

KAP AG

Vorstand