Fachliche & Technische Anforderungen zur Informationssicherheit

Februar 2024

Version 1/2024

Inhaltsverzeichnis

Grundlagen

1. Anwendungsbereich

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

Sie gilt in erster Linie für alle Fachabteilungen, die technische und organisatorische Maßnahmen umsetzen können. Hierzu gehören IT-Verantwortliche und Beschäftigte, Personalabteilung, Facility Management und vorübergehend Beschäftigte der IT des KAP-Konzerns sowie externe Dienstleister, die in diesen Bereichen konzernintern eingesetzt sind („**Mitarbeiter**“).

Die Richtlinie ist eine Ergänzung zur Informationssicherheitsrichtlinie und der Richtlinie für Anforderungen zur Informationssicherheit für Mitarbeiter und Vorgesetzte, 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 Richtlinie zur Informationssicherheit definiert, ist Informationssicherheit der Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen in jeglicher Form.

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

Diese Richtlinie gilt für alle (IT) Systeme, unabhängig davon ob intern entwickelt oder extern zugekauft.

2. Anforderungen an das Informationsmanagement

Informationseigentümer tragen die Verantwortung, dass die von Ihnen erstellten Informationen nach ihrer Vertraulichkeit klassifiziert werden.

Alle Informationen, unabhängig von ihrer Form, müssen auf der Grundlage der Ihnen zugewiesenen Klassifizierung geschützt werden.

Der Schutz und das Management von Informationen konzentrieren sich auf die Festlegung des Schutzniveaus von Informationsgütern und den daraus resultierenden Anforderungen.

Maßnahmen müssen definiert sein um dieses Schutzniveau während des kompletten Lebenszyklus aufrecht zu erhalten. Dies umfasst den Schutz bei der Übertragung, im Ruhezustand und die Anwendung geeigneter Zugangskontrollen.

2.1 Schutz von Informationen während des kompletten Lebenszyklus

2.1.1 Vorgaben müssen definiert sein, um dem Informationseigentümer zu ermöglichen seine Informationen sachgemäß in punkto Vertraulichkeit zu klassifizieren

2.1.2 Bei diesen Vorgaben muss auch das Risiko in Betracht gezogen werden, welches sich durch Verlust oder Diebstahl ergibt und die Integrität der Daten beeinflusst

2.1.3 Es müssen Anforderungen durch die Organisation definiert sein, um die Verfügbarkeit von Informationen entsprechend sicher zu stellen. Dies hat Auswirkungen auf Backup und Kapazitätsmanagement Systeme

2.1.4 IT Security und ISB definieren die technischen Anforderungen für den Schutz vor Datenabfluss auf der Grundlage der Informationsklassifizierung

2.1.5 Unternehmensdaten dürfen nur auf autorisierter Hard- und Software vorhanden sein

2.1.6 Der Zugang zu Unternehmensdaten muss eingeschränkt sein auf identifizierte, berechtigte und autorisierte Personen

2.1.7 Informationen müssen während des Transports, entsprechend ihrer Klassifizierung, durch Verschlüsselung geschützt werden:

a) In öffentlichen Bereichen und Netzwerken, wenn intern oder höher klassifiziert

b) Immer, wenn als streng vertraulich klassifiziert

c) Um Datenverlust durch verlorene und gestohlene Geräte zu verhindern, müssen mobile Geräte durch Verschlüsselung geschützt werden

2.1.8 Informationen oder IT Systeme die nicht mehr gebraucht werden müssen nach einem „Sicheren“ Verfahren gelöscht oder zerstört werden

2.1.9 Kontrollieren von Kommunikation und Verteilung von Informationen

2.1.10 IT Security, in Zusammenarbeit mit dem ISB, müssen zum Schutz vor ungewolltem Abfluss von Daten, Strategien entwickeln und ein System implementieren, um ausgehende Kommunikation zu überwachen und zu kontrollieren.

2.1.11 Externe Kommunikationskanäle müssen überwacht werden um Datenverlust und die Verbreitung von unangemessenem Inhalt zu verhindern.

2.1.12 Nicht autorisierte Kommunikationskanäle müssen identifiziert und deaktiviert werden.

2.1.13 Wo externe Kommunikationskanäle von Applikationen nicht deaktiviert sind, müssen Maßnahmen zum Schutz vor Datenverlusten getroffen werden.

2.1.14 Websites mit unangemessenem oder illegalem Inhalt müssen gesperrt werden

2.1.15 Basierend auf der Klassifizierung von Informationen müssen die Anforderungen und der Risiko Appetit für den Schutz vor Datenverlusten definiert werden.

2.1.16 Risiken und Ausnahmen müssen innerhalb eines akzeptablen Niveaus gemanagt werden. Die Bewertung von Cyber- und Informationssicherheitsrisiken und die Wirksamkeit von Gegenmaßnahmen müssen mit der Strategie des Risikorahmens und der Risikobereitschaft übereinstimmen

3. IT-Asset Management

Jede Transaktion von und mit Informationen hängt von der Sicherheit unserer Infrastruktur ab. Ein IT-Asset-Management ist eine Reihe von Praktiken, die sicherstellen, dass IT-Assets während ihres gesamten Lebenszyklus ordnungsgemäß verwaltet werden.

Das Asset Inventar muss regelmäßig überprüft und aktualisiert werden. Im Rahmen von Änderungen an der IT Infrastruktur muss die Aktualisierung des IT Asset Register ein fester Bestandteil der Planungs- und Umsetzungsarbeiten sein.

IT-Asset-Manager müssen IT-Assets erfassen und folgende Angaben dokumentieren:

a) Relevante Cyber- und Informationssicherheitsparameter, basierend auf der Klassifizierung nach der Vertraulichkeit, Integrität und Verfügbarkeit des Assets
b) Für ein wirksames technisches Schwachstellenmanagement muss das Inventar den Softwarehersteller, den Softwarenamen, die Versionsnummern und den aktuellen Stand der Bereitstellung beinhalten
c) Die Prozessbedingten Abhängigkeiten zwischen Anwendungen, Softwarepaketen und der Infrastruktur, die sie zum Betrieb benötigen

3.1 Standardisierte und einheitliche Inventarisierung

3.1.1 Die Inventarisierung beinhaltet alle im Unternehmen vorhandenen Hard- und Softwaredaten, ob physisch, virtuell, mobil oder in der Cloud

3.1.2 Die Inventarisierung muss einheitlich, standardisiert mittels geeigneter Tools erfolgen

3.2 Verantwortlichkeiten und Zuordnung

3.2.1 Jedes IT-Asset muss einen definierten IT-Asset Besitzer haben, der für das Asset verantwortlich ist. Das Eigentum an IT-Assets muss dokumentiert, verwaltet und aktualisiert werden, besonders wenn die Eigentümer das Unternehmen wechseln oder verlassen.

3.2.2 IT-Verantwortliche nominieren einen IT Asset Manager für ihren Verantwortungsbereich.

3.2.3 Das zentrale IT-Management muss einen Datenqualitätsprozess definieren und verwalten

3.3 Schutz vor unbefugtem Zugriff, Veränderung oder Zerstörung

3.3.1 Systeme und Infrastrukturen müssen vor unbefugtem Zugriff, Veränderung oder Zerstörung geschützt werden

3.3.2 Unbefugte IT-/IoT-Geräte müssen durch ein Verfahren im Netz erkannt und isoliert werden

3.3.3 Erkannte, unbefugte Geräte müssen genehmigt oder so schnell wie möglich entfernt werden

3.4 Regeln für die sichere Nutzung von Informationen und IT-Assets

3.4.1 Für das Unternehmen genutzte mobile Endgeräte wie Smartphones, Tablets und Laptops müssen mit einem Management System verwaltet werden. Die Verwaltung umfasst das Aktualisieren von Software und von Geräteeinstellungen, das Überwachen der Einhaltung von Organisationsrichtlinien sowie das Löschen oder Sperren von Geräten per Fernzugriff

3.4.2 Software oder andere Komponenten dürfen nicht heruntergeladen, installiert, eingesetzt oder verwendet werden, wenn sie nicht für das Unternehmen lizenziert sind.

3.4.3 Standardmäßig müssen alle Protokolle und Dienste, die nicht ausdrücklich für die Nutzung über das Internet zugelassen sind, gesperrt werden

3.4.4 Es muss ein Verfahren zur angemessenen Kontrolle und Steuerung der Internetnutzung und anderer externer Verbindungen vorhanden sein

3.4.5 Zwischen dem Internet und den internen Netzen muss eine Firewall-Infrastruktur etabliert sein, dies gilt ebenso für Cloud Umgebungen

3.5 Gewährleistung eines sicheren und belastbaren Betriebes

3.5.1 Die Konfigurationseinstellungen, die für die Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Infrastrukturkomponenten relevant sind, müssen definiert, getestet und genehmigt werden, bevor sie in der Produktion bereitgestellt werden

3.5.2 Die Konfigurationseinstellungen müssen regelmäßig überprüft und aktualisiert werden, um sie an Änderungen der zugrunde liegenden Sicherheitsanforderungen anzupassen

3.5.3 Änderungen an Firewall-Regeln müssen genehmigt und einem definierten Change-Management-Prozess unterzogen werden. Regelmäßig, mindestens einmal jährlich, müssen diese Regeln validiert und ggfs. entfernt werden

3.5.4 Wenn Sicherheitszertifikate verwendet werden, muss sichergestellt sein, dass ein Prozess zur Überwachung und Erneuerung von Zertifikaten vorhanden ist

3.5.5 Der Lebenszyklus von Anwendungen und Infrastrukturkomponenten muss verwaltet werden, um diejenigen zu identifizieren, die sich dem Ende ihrer Lebensdauer nähern, um Sicherheitspatches oder Hotfixes bereitzustellen

3.5.6 Für End-of-Life-Lösungen, die nicht mehr von dem entsprechenden Drittanbieter unterstützt werden, müssen zusätzliche Kontrollen eingerichtet werden, um ein akzeptables Risikoniveau aufrechtzuerhalten.

3.5.7 Informationen über technische Schwachstellen verwendeter Systeme sollten rechtzeitig eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen bewertet und angemessene Maßnahmen ergriffen werden, um das dazugehörige Risiko zu behandeln. Dazu gehört:

a) Aufgaben und Verantwortlichkeiten festzulegen und einrichten, die die Überwachung auf Schwachstellen, die Risikobeurteilung von Schwachstellen, das Einspielen von Patches, die Nachverfolgung von Assets und sämtliche erforderlichen Koordinationsaufgaben umfassen;

b) ein Zeitplan zur Reaktion über möglicherweise relevante technische Schwachstellen. Hochrisikosysteme sollten bevorzugt behandelt werden;

c) Patches sollten vor der Installation getestet und beurteilt werden, um unerwünschte Nebeneffekte auszuschließen

d) Steht kein Patch zur Verfügung, sollten andere Maßnahmen in Betracht gezogen werden:

i. Abschaltung der Dienste/Funktionen, die durch Schwachstelle betroffen sind
ii. Anpassung der Zugriffssteuerung, z.B. Firewalls, an Netzwerkgrenzen
iii. Verstärkte Überwachung zur Erkennung stattfindender Angriffe
iv. Sensibilisierung der Beschäftigte für die Schwachstelle
v. Alle durchgeführten Maßnahmen sollten in einem Protokoll vermerkt werden

3.5.8 Erkennungs-, Vorbeugungs- und Wiederherstellungsmaßnahmen zum Schutz vor Schadsoftware müssen umgesetzt werden und beinhalten u.a.

a) Installation und regelmäßige Aktualisierung einer Schadsoftware-Erkennungs- und Reparatur-Software zum routinemäßigen Scannen von Computern und Medien

b) Untersuchung aller über Netzwerke empfangener oder über ein Speichermedium erhaltener Dateien auf Schadsoftware vor der Verwendung;

c) Untersuchung von E-Mail-Anhängen und heruntergeladenen Dateien auf Schadsoftware vor der Verwendung

3.6 Netzwerksicherheit

3.6.1 Netzwerkverbindungsaktivitäten müssen überwacht und kontrolliert werden, um Sicherheitsvorfälle auf der Grundlage definierter Bedrohungsanwendungsfälle zu identifizieren und zu eskalieren

3.6.2 Netzwerkverbindungen dürfen nur für zugelassene und authentifizierte Segmente, Personen und Geräte gemäß den Anforderungen an die Zugriffsverwaltung zugelassen werden

3.6.3 Netzwerkverbindungen, die über öffentliche Netzwerke laufen, müssen verschlüsselt sein

3.6.4 Die Dokumentation sensibler Netzwerkeinstellungen muss gespeichert, auf dem neuesten Stand gehalten und nach dem Least-Privilege-Prinzip verfügbar sein

3.6.5 Netzwerkdiagramme sind streng vertraulich und müssen gepflegt werden, um eine schnellere Wiederherstellung von Systemen im Falle von Sicherheitsvorfällen zu ermöglichen

3.6.6 Benutzer sollten ausschließlich Zugang auf diejenigen Netzwerke und Netzwerkdienste haben, zu deren Nutzung sie ausdrücklich befugt sind

3.7 Datensicherung und Wiederherstellung

3.7.1 Systeme, Anwendungen und Daten müssen gemäß dokumentierter Sicherungs- und Wiederherstellungsanforderungen gesichert werden

3.7.2 Es sollte eine Richtlinie erstellt werden, wo grundlegende Sicherungs- und Wiederherstellungsanforderungen, sowie Aufbewahrungs- und Schutzanforderungen festgelegt sind

3.7.3 Es sollten angemessene Datensicherungseinrichtungen vorhanden sein, um zu gewährleisten, dass alle wichtigen Informationen und Anwendungen nach einem Vorfall oder Medienausfall wiederhergestellt werden können

3.7.4 Bei der Aufstellung eines Datensicherungs-Plans sollten die folgenden Punkte in Betracht gezogen werden**:**

a) Es sollten genaue und vollständige Aufzeichnungen der Datensicherungskopien und der dokumentierten Wiederherstellungsverfahren erstellt werden

b) Es sollte eine Übersicht geführt werden, in dem Speicherort und Inhalt der Datensicherungen aufgeführt sind

c) Umfang (z. B. komplette oder differentielle Datensicherung) und Häufigkeit der Datensicherungen sollten den geschäftlichen Anforderungen der Organisation, den Sicherheitsanforderungen bezüglich der betreffenden Informationen und der Wichtigkeit der Information für die Fortführung der Betriebstätigkeit entsprechen

d) die Datensicherungen sollten an einem externen Ort in ausreichender Entfernung aufbewahrt werden, um vor Schäden am Hauptstandort geschützt zu sein

e) die Datensicherungsinformationen sollten über einen angemessenen Schutz vor physischen und Umweltfaktoren verfügen, der den am Hauptstandort angewandten Normen entspricht

f) Datensicherungen sollten regelmäßig überprüft werden, um sicherzustellen, dass auf sie im Notfall Verlass ist. Dies sollte zusammen mit einer Überprüfung der Wiederherstellungsverfahren in Verbindung mit einer Überprüfung der für die Wiederherstellung benötigten Zeit erfolgen

g) Im Rahmen der Betriebsabläufe sollten die Durchführung von Datensicherungen überwacht und Maßnahmen bei fehlgeschlagenen Datensicherungen festgelegt werden, um die Vollständigkeit der Backups zu gewährleisten

h) In Situationen, in denen Vertraulichkeit besonders wichtig ist, sollten die Datensicherungen mittels Verschlüsselung geschützt werden.

4. Identitäts- und Berechtigungsmanagement

Der Zugang zu schützenswerten Ressourcen ist auf berechtigte Benutzer und berechtigte IT-Komponenten einzuschränken. Benutzer und IT-Komponenten müssen zweifelsfrei identifiziert und authentisiert werden. Das Berechtigungsmanagement ist die Kontrolle des Zugangs zu unseren Informationen, Systemen, Dienstleistungen und Räumlichkeiten.

4.1 Zugriffsrechte / Logische Zugriffe

4.1.1 Es muss einen Prozess geben zur effektiven Verwaltung und der Berechtigungsvergabe für neue Mitarbeiter (Joiners), Mitarbeiter, die wechseln (Movers) und Mitarbeiter, die die Firma verlassen (Leavers), dieser beinhaltet:

a) Sofortige Deaktivierung des Zugriffs oder Löschung der Kennungen von Benutzern, die die Organisation verlassen haben
b) Regelmäßige Identifizierung und Löschung oder Deaktivierung überflüssiger Benutzerkennungen
c) Sicherstellung, dass ehemals genutzte Kennungen nicht an andere Benutzer vergeben, werden
d) Der Prozess muss Benachrichtigungen und ein Genehmigungsverfahren ermöglichen

4.1.2 Die Vergabe und Verwaltung von Benutzerrechten erfolgt gemäß vorhandener Berechtigungskonzepte und Richtlinien

4.1.3 Benutzerkonten dürfen nur einer Person zugeordnet sein und es ist generell nicht gestattet Benutzerkonten mit anderen Personen zu teilen

4.1.4 Berechtigungen sollen sich auf die Mindestanforderungen beschränken, d.h. nach dem Least-Privilege-Prinzip

4.1.5 Berechtigungen dürfen nur bereitgestellt werden, wenn sie ordnungsgemäß genehmigt wurden und mit dem definierten Genehmigungsworkflow übereinstimmen

4.1.6 Der privilegierte Zugriff darf für gültige Anwendungsfälle aktiviert und genutzt werden

4.1.7 Aktivitäten von Konten mit privilegiertem Zugriff auf die Produktionsumgebung müssen protokolliert werden, um die Überprüfbarkeit und Sicherheitsüberwachung zu unterstützen

4.1.8 Die Standardeinstellung ist kein Zugriff auf lokale Administratorrechte für Workstations. Ausnahmen dürfen nur für temporäre, administrative Zugriffe gewährt werden, die durch einen gültigen Anwendungsfall unterstützt werden

4.1.9 Für IT-Mitarbeiter sind folgende Anwendungsfälle genehmigt:

a) Integration von Drittanbieter Software
b) Support Aufgaben, die nicht mit Standard Tools durchgeführt werden können
c) Software-Evaluierung und System Installation

4.1.10 Nicht personenbezogene, technische Konten müssen:

a) In einem Repository registriert sein und einem Eigentümer zugeordnet sein
b) Sie müssen sicher konfiguriert sein um unbefugte Nutzung zu verhindern, d.h. die Anforderung an sichere Passwörter erfüllen, mit dem Verbot der Offenlegung, bei beschränkter Verteilung für autorisiertes Personal

4.1.11 Eingebaute Standardkonten von Drittanbieter Produkten müssen deaktiviert sein, wo dies nicht möglich ist, muss das Initialpasswort umgehend geändert werden

4.1.12 Es muss ein Prozess definiert werden, der Anwendungsfälle und die erforderliche Genehmigungsstufe für den Zugriff auf die Daten einer anderen Person (aktiv oder ehemalig) festlegt. Dieser Prozess wird in Abstimmung mit der Personalabteilung und der Rechts- und Compliance-Abteilung in Bezug auf die gesetzlichen Anforderungen dokumentiert. Die IT-Abteilung muss diesen Prozess implementieren, um sicherzustellen, dass die erforderlichen Daten zur Verfügung gestellt werden können.

4.2 Authentifizierung

4.2.1 Es muss ein geeignetes Authentifizierungsverfahren zur Bestätigung der Identität des Benutzers gewählt werden.

4.2.2 Für eine starke Authentifizierung und Identitätsverifizierung (Multi-faktor) müssen Authentifizierungsalternativen zu Kennwörtern wie kryptographische Verfahren, Smartcard oder Token verwendet werden

4.3 Sichere Anmeldeverfahren

4.3.1 Ein gutes, sicheres Anmeldeverfahren sollte:

a. keine System- oder Anwendungsidentifikatoren anzeigen, bis der Anmeldeprozess erfolgreich abgeschlossen wurde
b. eine allgemeine Warnmeldung anzeigen, dass nur befugte Benutzer Zugang zum System haben sollten
c. während des Anmeldeverfahrens keine Hilfetexte anzeigen, die sich Unbefugte zunutze machen könnten
d. die Anmeldedaten erst nach Eingabe aller Daten überprüfen
e. Bei Auftreten eines Fehlers sollte das System nicht anzeigen, welcher Teil der eingegebenen Daten richtig / nicht richtig war
f. vor Brute-Force-Anmeldeversuchen schützen;
g. erfolglose und erfolgreiche Anmeldeversuche protokollieren;
h. bei Erkennung einer möglicherweise versuchten oder erfolgreichen Umgehung der Anmeldesteuerung ein Sicherheitsereignis auslösen
i. das eingegebene Kennwort nicht anzeigen
j. Kennwörter nicht im Klartext über das Netzwerk übertragen
k. inaktive Sitzungen nach einer vorgegebenen Zeitspanne beenden, insbesondere an Hochrisiko-Standorten wie in öffentlichen oder externen Bereichen, die nicht dem Sicherheitsmanagement der Organisation unterstehen
l. bei kritischen Anwendungen Verbindungszeiten beschränken, um zusätzliche Sicherheit und möglichst wenig Gelegenheit für unbefugte Zugangsversuche zu bieten

4.3.2 Nach erfolgreicher Anmeldung sollten die folgenden Daten angezeigt werden:

a) Datum und Uhrzeit der letzten erfolgreichen Anmeldung
b) Einzelheiten zu erfolglosen Anmeldeversuchen seit der letzten erfolgreichen Anmeldung

4.3.3 Der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, muss eingeschränkt und streng überwacht werden

5. Physische und umgebungsbezogene Sicherheit

Unbefugter Zutritt, die Beschädigung und die Beeinträchtigung von Information und informationsverarbeitenden Einrichtungen der Organisation müssen verhindert werden. Verlust, Beschädigung, Diebstahl oder Gefährdung von Werten und die Unterbrechung von Organisationstätigkeiten sind zu unterbinden. Sicherheitsbereiche müssen identifiziert und entsprechend dokumentiert werden.

5.1 Physische Sicherheitsperimeter

5.1.1 In einem Gebäude oder Standort, in denen sich Einrichtungen zur Verarbeitung von Informationen befinden, gelten Sicherheitsanforderungen, die von den Informationswerten und den Ergebnissen einer Risikoeinschätzung abhängen sollten

5.1.2 Physischen Zugänge zu Standorten bzw. Gebäuden müssen gesichert und kontrolliert werden, der Zutritt darf nur befugten Personen gestattet werden

5.1.3 der Organisation unterstehende Einrichtungen zur Informationsverarbeitung sollten physisch von jenen Einrichtungen getrennt sein, die von externen Parteien verwaltet werden

5.1.4 es sollten geeignete, Normen entsprechende Einbruchmeldeanlagen installiert und regelmäßig überprüft werden

5.1.5 Brandschutztüren in Sicherheitsbereichen sollten über Alarmvorrichtungen verfügen sowie überwacht und überprüft werden

5.2 Physische Zutrittssteuerung

5.2.1 Sicherheitsbereiche sollten durch eine angemessene Zutrittssteuerung geschützt werden um sicherzustellen, dass nur berechtigtes Personal Zutritt hat.

5.2.2 An- und Abmeldung von Besuchern sollten mit Datum und Uhrzeit vermerkt werden, und alle Besucher sollten beaufsichtigt werden, sofern ihr Aufenthalt nicht zuvor genehmigt wurde.

5.2.3 Besuchern sollte der Zutritt nur für spezifische, genehmigte Zwecke gestattet werden, und sie sollten bezüglich der Sicherheitsanforderungen im betreffenden Bereich sowie der Notfallmaßnahmen eingewiesen werden. Die Identität der Besucher sollte auf geeignete Weise bestätigt werden;

5.2.4 der Zutritt zu Bereichen, in denen vertrauliche Informationen verarbeitet oder gespeichert werden, sollte mittels geeigneter Zutrittssteuerungen wie z. B. eines aus einer Zutrittskarte und einer geheimen PIN bestehenden Zwei-Faktor-Authentifizierungsmechanismus befugten Personen vorbehalten werden

5.2.5 es sollten ein physisches oder ein elektronisches Protokoll existieren, welche sicher aufbewahrt und überwacht werden

5.2.6 alle Beschäftigte, Auftragnehmer und externe Parteien sollten verpflichtet werden, ein gut sichtbares Erkennungszeichen in den Standorten bzw. Gebäuden zu tragen

5.2.7 Beschäftigten externer Support-Dienstleister sollte nur dann beschränkter Zutritt zu Sicherheitsbereichen oder Einrichtungen zur Verarbeitung vertraulicher Informationen gewährt werden, wenn dies erforderlich ist. Dieser Zutritt sollte eigens genehmigt und überwacht werden

5.2.8 Zutrittsrechte in Bezug auf Sicherheitsbereiche sollten regelmäßig überprüft und aktualisiert sowie, sofern erforderlich, wieder entzogen werden

5.3 Arbeiten in Sicherheitsbereichen

5.3.1 Die Beschäftigten sollten nur im Bedarfsfall über die Existenz eines Sicherheitsbereichs bzw. dort stattfindende Aktivitäten unterrichtet werden

5.3.2 Aus Sicherheitsgründen und zur Unterbindung böswilliger Handlungen sollten unbeaufsichtigte Tätigkeiten in Sicherheitsbereichen vermieden werden

5.3.3 Ungenutzte Sicherheitsbereiche sollten unter Verschluss gehalten und regelmäßig überprüft werden

5.3.4 Das Mitführen von Foto-, Video-, Audio- und sonstigen Aufzeichnungsgeräten wie Mobiltelefonen mit Kameras sollte untersagt und nur nach ausdrücklicher Genehmigung gestattet werden

5.4 Anlieferungs- und Ladebereiche

5.4.1 Zutrittsstellen wie Anlieferungs- und Ladebereiche sowie andere Stellen, über die unbefugte Personen die Räumlichkeiten betreten könnten, sollten überwacht und, falls möglich, von informationsverarbeitenden Einrichtungen getrennt werden, um unbefugten Zutritt zu verhindern

5.4.2 Eingehendes Material sollte entsprechend der Verwaltung der Werte beim Eingang am Standort registriert werden und auf Manipulationen während des Transports untersucht werden. Sofern sich Anzeichen für Manipulationen finden, sollten diese unverzüglich dem Sicherheitspersonal gemeldet werden

6. Personalsicherheit

Alle Personen, die sich um eine Stelle bewerben, sollten einer Sicherheitsüberprüfung unterzogen werden. Diese Überprüfung muss im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen sein. Ein angemessenes Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken ist notwendig.

6.1 Sicherheitsüberprüfung

6.1.1 Überprüfungen sollten alle Rechtsvorschriften über Datenschutz, Schutz der Privatsphäre und arbeitnehmerrelevante Gesetzgebung berücksichtigen und, sofern erlaubt, folgendes einschließen:

a) Zufriedenstellende Leumundszeugnisse, z.B. ein dienstliches Zeugnis
b) Ein auf Vollständigkeit und Richtigkeit geprüfter Lebenslauf des Bewerbers
c) Bestätigung angegebener akademischer und beruflicher Qualifikationen
d) Unabhängige Identitätsüberprüfung (Reisepass oder ähnliches Dokument)

6.1.2 Wenn eine Person für eine bestimmte Rolle der Informationssicherheit angestellt wird, sollten Organisationen sicherstellen, dass der Bewerber:

a) Über die notwendige Kompetenz für die Aufgabe verfügt
b) Über die erforderliche Vertrauenswürdigkeit verfügt, insbesondere wenn die Rolle von entscheidender Bedeutung für die Organisation ist

6.2 Beschäftigungs- und Vertragsbedingungen

In den vertraglichen Vereinbarungen mit Beschäftigten und Auftragnehmern sollten deren Verantwortlichkeiten und diejenigen der Organisation festgelegt werden.

6.3 Aus- und Weiterbildung in Informationssicherheit

Alle Mitarbeiter der Organisation sollten ein angemessenes Bewusstsein bekommen durch Ausbildung und Schulung sowie regelmäßige Aktualisierungen zu den Richtlinien und Verfahren der Organisation, die für ihr berufliches Arbeitsgebiet relevant sind.

6.3.1 Ein Sensibilisierungsprogramm für Informationssicherheit sollte darauf abzielen, dass sich Mitarbeiter ihrer Verantwortung für Informationssicherheit bewusst werden

6.3.2 Aus- und Weiterbildung zur Informationssicherheit sollte regelmäßig stattfinden. Eine anfängliche Aus- und Weiterbildung gilt nicht nur für Neuanfänger, sondern auch für Beschäftigte, die in andere Positionen oder Funktionen mit deutlich unterschiedlichen Anforderungen an Informationssicherheit versetzt wurden

6.3.3 Aus- und Weiterbildung in Informationssicherheit sollte generelle Aspekte enthalten wie:

a) Darlegung der Verpflichtung der Leitung zur Informationssicherheit in der Organisation
b) Die Notwendigkeit, mit geltenden Regeln und Verpflichtungen der Informationssicherheit vertraut zu werden und sie zu beachten
c) Persönliche Verantwortung für eigene Handlungen und Unterlassungen, sowie Verantwortlichkeiten zum Schutz von Informationen die der Organisation gehören

d) Grundsätzliche Verfahren zur Informationssicherheit (wie Berichterstattung über Informationssicherheitsvorfälle) und grundlegende Sicherheitsmaßnahmen (wie Kennwortsicherheit, Maßnahmen bei Schadsoftware und „clear desk“)
e) Anlaufstellen und Ressourcen für zusätzliche Informationen, Empfehlungen und Fragen, sowie Aus- und Weiterbildungsunterlagen zur Informationssicherheit

6.4 Maßregelungsprozess

6.4.1 Ein klarer und transparenter Maßregelungsprozess sollte eingerichtet sein, um Maßnahmen zu ergreifen, wenn ein Informationssicherheitsverstoß begangen wurde

6.4.2 Ein Maßregelungsprozess sollte nicht ohne vorherige Prüfung eingeleitet werden, ob tatsächlich eine Informationssicherheitsverletzung aufgetreten ist

6.4.3 Ein formeller Maßregelungsprozess sollte eine korrekte und faire Behandlung sicherstellen

6.5 Beendigung und Änderung der Beschäftigung

6.5.1 Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, sollten festgelegt, dem Beschäftigten mitgeteilt und durchgesetzt werden

6.5.2 Die nach Beendigung des Arbeitsverhältnisses weitergeltenden Verantwortlichkeiten und Pflichten sollten in den Beschäftigungsbedingungen beschrieben werden

6.5.3 Änderungen bei Verantwortung oder Beschäftigung sollten genauso geregelt werden wie die Beendigung aktueller Verantwortung oder Beschäftigung

7. Verwendung von Passwörtern

Da Passwörter auch ausgespäht und entschlüsselt werden können, müssen bestimmte Regeln beachtet werden, um ein sicheres Passwort zu gewährleisten.

Die folgenden Passwortregeln sind unter diesen Sicherheitsanforderungen erarbeitet worden und bieten bei einer konsequenten Anwendung ein hohes Maß an Sicherheit

7.1 Passwortregeln

7.1.1 Jeder PC-Benutzer ist verpflichtet, ihm zur Verfügung gestellte bzw. von ihm benutzte Passwörter vertraulich zu behandeln und geheim zu halten, sodass sie Dritten nicht zugänglich sind. Passwörter dürfen nicht an Dritte, nicht an Kolleginnen und Kollegen und auch nicht an IT-Administratoren weitergegeben werden

7.1.2 Passwörter dürfen nicht in Dateien oder Skripten gespeichert und auch nicht am Arbeitsplatz, z. B. auf Zetteln, hinterlegt oder auf Funktionstasten gespeichert werden

7.1.3 Die Anmeldung darf niemals unter einem fremdem Benutzernamen/Passwort erfolgen

7.1.4 Bei einem Verdacht auf Verlust der Vertraulichkeit oder Ausspähung ist das Passwort sofort zu ändern. Ansonsten sind Passwörter in Abständen von 180 Tagen zu ändern Es ist ein von den bisher genutzten Passwörtern abweichendes Passwort zu wählen

7.1.5 Voreingestellte Passwörter (z. B. des Herstellers oder der IT-Administration bei Auslieferung/Installation von Systemen) dürfen nur einmalig verwendbar sein und sind unverzüglich durch individuelle Passwörter zu ersetzen

7.1.6 Bereits benutzte Passwörter dürfen nach einem Passwortwechsel nicht wiederverwendet werden

7.1.7 Passwörter sind verdeckt einzugeben, um eine Kenntnisnahme durch Unbefugte zu verhindern

7.1.8 Bei Verdacht von Missbrauch ist unverzüglich die IT-Systemadministration einzuschalten

7.1.9 Das Passwort muss mindestens 8 Zeichen lang sein. Es muss aus Groß- und Kleinbuchstaben und mindestens aus einer Ziffer und einem Sonderzeichen (z. B.*“§$%& etc.) bestehen und darf nicht mehr als zwei aufeinanderfolgende identische Zeichen enthalten

7.1.10 Es dürfen keine Trivialpasswörter verwendet werden, dazu gehören aufeinanderfolgende Buchstaben und Zahlen, z. B.123456 oder abcdefg oder aufeinanderfolgende Tastaturzeichen, z. B. asdfgh

7.1.11 Es dürfen auch keine Passwörter verwendet werden, die mit dem einzelnen Mitarbeiter in Verbindung gebracht werden können, z. B. Name, Wohnort, Kfz-Kennzeichen etc., und keine Namen/Begriffe, die in Wörterbüchern stehen können

7.1.12 Die Benutzerkennung darf nicht Bestandteil des Passworts sein

7.1.13 Die von einigen Browsern angebotene Funktion „Passwort speichern“ darf nicht verwendet werden

7.1.14 Passwörter, welche innerhalb des Unternehmens verwendet werden, dürfen nicht in anderen Umgebungen (z. B. im Internet, auf Kundenportalen etc.) gleichlautend verwendet werden

7.1.15 Um im Fall einer Kompromittierung des Passworts die Risiken möglichst gering zu halten, sollte auch innerhalb des Unternehmens für mehrere Zugänge bzw. Applikationen nicht das gleiche Passwort verwendet werden

7.1.16 Nach einer mehrmaligen Falscheingabe (drei bis fünf Fehlversuche) ist der Zugang zu blockieren und darf erst nach einer zweifelsfreien Identifikation des Benutzers wieder freigegeben werden

Die Einhaltung dieser Passwortregeln ist in einem ausreichenden Umfang **automatisiert** zu kontrollieren und zu erzwingen.

8. Informationssicherheit in Beziehungen mit Dritten (Third Party)

Während wir Drittparteien („third parties“) wie z. B. Lieferanten, Dienstleister, Berater oder Distributoren, zur Unterstützung und Erbringung von Dienstleistungen für Geschäftsfunktionen im gesamten Unternehmen einsetzen, können wir unsere Verantwortung für den Schutz von Informationen nicht delegieren. Cyber- und Informationssicherheitsanforderungen in Bezug auf Aktivitäten Dritter und Lieferketten sind unerlässlich, um unserer Verpflichtung nachzukommen, unsere Informationen in jeglicher Form zu schützen. Das gilt im Besonderen, wenn der Dritte Daten speichert oder überträgt oder wenn wir eine Netzwerkverbindung mit dem Dritten hergestellt haben.

8.1 Third Party Cyber- und Informationssicherheitsanforderungen

8.1.1 Maßnahmen zu Cyber- und Informationssicherheitsanforderungen müssen festgelegt und angeordnet werden, um spezifisch den Zugriff von Dritten auf die Informationen der Organisation zu regeln. Dazu zählen:

a) Eine Bewertung von Cyber- und Informationssicherheitskontrollen muss Bestandteil des Auswahlverfahrens für Dritte sein, eingeleitet durch die Geschäftsfunktion die einen Dritten beauftragen möchte
b) Mindestanforderungen an die Informationssicherheit für jede Informations- und Zugriffsart als Grundlage für die einzelnen Verträge, entsprechend den geschäftlichen Bedürfnissen, Anforderungen und dem Risikoprofil
c) Feststellung und Dokumentation der Arten Drittanbieter, z. B. IT-Dienstleistungen, Logistik und Versorgungseinrichtungen
d) ein standardisierter Prozess und Lebenszyklus zum Management der Drittanbieterbeziehung

e) Festlegung der jeweiligen Art und Weise des Informationszugriffs sowie Überwachung und Kontrolle des Zugriffs
f) Genauigkeits- und Vollständigkeitskontrollen zur Sicherstellung der Integrität der Informationen bzw. der von den einzelnen Parteien vorgenommenen Informationsverarbeitung
g) Es muss eine zyklische Überprüfung der vereinbarten Kontrollen durchgeführt werden, auf der Grundlage eines wiederholbaren und messbaren Bewertungsmechanismus
h) Regelungen für den Umgang mit Vorfällen und Gefahren im Zusammenhang mit dem Lieferantenzugriff einschließlich Verantwortlichkeiten auf beiden Seiten,
i) Vorkehrungen bezüglich Ausfallsicherheit sowie ggf. zur Wiederherstellung und für den Notfall, um die Verfügbarkeit der Informationen bzw. der von den einzelnen Parteien vorgenommenen Informationsverarbeitung sicherzustellen
j) Management der erforderlichen Übergabe von Informationen, informationsverarbeitenden Einrichtungen u. a. und Sicherstellung, dass die Informationssicherheit während der gesamten Übergabephase gewahrt bleibt.
k) Für geplante sowie ungeplante Beendigungen der Vertragsverhältnisse müssen Regelungen getroffen werden, in denen festgelegt wird, wie alle Informationen, Daten und Hardware der Nutzenden von Dritten zurückgegeben werden (Beendigungskonzept)

8.2 Third Party Risikomanagement

8.2.1 Vor Abschluss eines Vertrags mit einem Dritten, der Dienstleistungen oder Produkte für uns erbringt, muss eine Risikobewertung der Cyber- und Informationssicherheitskontrollen des Dritten durchgeführt werden, die dem Risiko entspricht, das von der Nutzung des Dritten ausgeht

8.2.2 Mittels einer Analyse auf Basis einer Bewertung etwaiger Risiken und deren Klassifizierung, muss geklärt werden, ob die auszulagernde Aktivität oder der auszulagernde Prozess unter Risikogesichtspunkten mit einem hohen Risiko für das Institut zu bewerten ist und eventuell weitere Maßnahmen zu ergreifen sind

9. Inkrafttreten

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

KAP AG

Vorstand