[Name der Organisation]

ST4 Mitarbeiterhandbuch Informationssicherheit

Version	**1.0**
Eigentümer der Richtlinie	Name eintragen
Geprüft von	Name oder Rolle eintragen
Prüfdatum	Datum eintragen
Gültig ab	Datum eintragen
Nächste Überprüfung	Datum eintragen
Vertraulichkeitsklasse	INTERN

Änderungsverlauf

Datum	**Version**	**Erstellt von**	**Beschreibung der Änderung**
27.05.25	0.92	DataGuard	Grundstruktur des Dokuments
XX.XX.24	1.00	XX	Genehmigte Version und minimale Änderungen

[Wie diese DataGuard Richtlinienvorlage zu verwenden ist:]

[DataGuard möchte Ihnen einige wichtige Hinweise zur Anwendung der bereitgestellten Richtlinienvorlage geben. Diese Vorlage soll Ihnen als Ausgangspunkt dienen, um eigene, auf Ihre Organisation zugeschnittene Richtlinien zu entwickeln. Bitte beachten Sie die folgenden Hinweise zur Verwendung der Vorlage sorgfältig.

Verwendung der Vorlage

- **Vorlage als Ausgangspunkt:** Diese Vorlage ist sorgfältig recherchiert und von Experten zusammengestellt worden. Sie ist als Ausgangspunkt für die Erstellung Ihrer eigenen Richtlinie gedacht und bietet eine Struktur sowie Beispiele für Ihre künftiges Dokument. Bei allen Bemühungen erhebt diese Vorlage jedoch keinen Anspruch auf Passgenauigkeit und Vollständigkeit, denn die individuellen Gegebenheiten in Ihrer Organisation können abweichen.
- **Grundsatz der Effektivität:** Eine Richtlinie soll erforderlich, angemessen, passend, aufklärend und unterstützend für Ihren individuellen Unternehmenszweck wirken. Sorgen Sie dafür, dass Ihre Richtlinien stets diesem Grundsatz entsprechen.
- **Überprüfung der Inhalte:** Gehen Sie die Inhalte der Vorlage sorgfältig durch und überprüfen Sie diese im Hinblick auf die spezifischen Bedürfnisse und Anforderungen.
- **Vollständiges Verständnis erforderlich:** Stellen Sie sicher, dass Sie als Ersteller dieses Dokuments alle beschriebenen Anweisungen und Verfahren vollständig verstehen und für Ihre Organisation als anwendbar halten. Nur so können Sie fundierte Entscheidungen über Anpassungen treffen.
- **Klärung von Unklarheiten:** Sollten Sie auf Inhalte stoßen, die Sie nicht vollständig verstehen, holen Sie unbedingt weitere Informationen ein. Dies kann durch Rücksprache mit unseren DataGuard-Experten, rechtlichen Beratern oder anderen Fachexperten außerhalb oder innerhalb Ihrer Organisation geschehen.
- **Individuelle Anpassung erforderlich:** Die in der Vorlage beschriebenen Anweisungen und Verfahren sind pauschale Beispiele oder Vorschläge ohne tiefere Berücksichtigung Ihres Unternehmenskontextes. Daher ist es erforderlich, dass Sie den Inhalt der Richtlinien an die tatsächlichen Gegebenheiten und Anforderungen Ihrer Organisation anpassen.*
- **Keine ungeprüfte Übernahme:** Übernehmen Sie keine Texte oder Anweisungen aus der Vorlage, wenn diese nicht den spezifischen Anforderungen und der tatsächlichen Situation in Ihrer Organisation entsprechen. Jede Organisation ist einzigartig, und pauschale Übernahmen können zu Fehlern oder Missverständnissen führen.
- **Verantwortung der Geschäftsführung:** Beachten Sie, dass die endgültige Verantwortung für die Gestaltung und

Umsetzung von Richtlinien bei der obersten Leitung Ihrer Organisation liegt. Es ist entscheidend, dass diese alle Inhalte kritisch überprüft und eine Korrektur von unpassenden Inhalten veranlasst.]

[*) Die in dieser Vorlage gelb hinterlegten und in eckigen Klammern gesetzten Hilfstexte und Hinweise sollen nach Kennnisnahme eliminiert oder inhaltlich angepasst werden. Beispiel: Bitte eliminieren Sie diese Seite vor Veröffentlichung der Richtlinie.]

1 Einleitung

Willkommen zum Mitarbeiterhandbuch für Informationssicherheit der [Name der Organisation]. In der heutigen digitalen Welt ist der Schutz unserer Informationen - also aller Daten, die für unsere Organisation in einem bestimmten Kontext nützlich sind - von größter Bedeutung.

Dieses Handbuch bietet Ihnen alle wichtigen Richtlinien und Verfahren, die erforderlich sind, um die Vertraulichkeit, Integrität und Verfügbarkeit unserer wertvollen Informationen zu gewährleisten. Unser Ziel ist es, ein sicheres Arbeitsumfeld zu schaffen, in dem Informationen angemessen geschützt und Risiken minimiert werden.

Jede/r Mitarbeiter/in spielt eine wesentliche Rolle im Informationssicherheitsmanagement und trägt dazu bei, potenzielle Sicherheitsbedrohungen zu erkennen und zu vermeiden. Bitte lesen Sie die folgenden Seiten sorgfältig durch und stellen Sie sicher, dass Sie alle Richtlinien verstehen und einhalten. Ihr Engagement für Informationssicherheit ist entscheidend für den Erfolg und die Integrität unserer Organisation.

Erklärungen zu Fachbegriffen, die in unseren Richtlinien zur Informationssicherheit verwendet werden, sind in einem Glossar in [Bitte ergänzen Sie hier den Ort Ihres ISMS Glossars] erläutert. Bei weiteren Fragen oder Unsicherheiten stehen Ihnen Ihre Vorgesetzten sowie Ihre [IT- und Sicherheitsabteilung – Bitte erwähnen sie hier Ihre zuständige Abteilung]zur Verfügung. Gemeinsam können wir eine sichere und vertrauensvolle Arbeitsumgebung schaffen.

2 Gebrauch von Informationswerten

Um sicherzustellen, dass wir alle Informationen in unserem Unternehmen richtig nutzen und schützen, befolgen Sie bitte die folgenden Anweisungen:

1. **Interne Informationen:**
    a. Verwenden Sie interne Informationen nur für Ihre Arbeit und teilen Sie sie nicht mit Personen außerhalb des Unternehmens.
    b. Halten Sie sich an die im folgenden festgelegten Klassifizierungsstufen (Intern, vertraulich, streng vertraulich) und gehen Sie entsprechend vorsichtig mit den Daten um.
    c. Speichern Sie interne Informationen sicher und geben Sie den Zugang nur an berechtigte Personen frei.
2. **Externe Informationen:**
    a. Behandeln Sie externe Informationen, die uns von Partnern oder Kunden zur Verfügung gestellt werden, mit der gleichen Sorgfalt wie unsere internen Informationen.
    b. Stellen Sie sicher, dass alle externen Informationen, die vertraulich sind, gemäß den Anforderungen der jeweiligen Partner oder Kunden geschützt werden.
    c. Teilen Sie keine externen Informationen ohne ausdrückliche Erlaubnis weiter.
    d. Nutzen Sie externe Informationssysteme (Software, Cloud-Systeme etc.) ausschließlich entsprechend den Nutzungsanweisungen bzw. Herstellerspezifikationen. Das betrifft insbesondere die Speicherung von klassifizierten Informationen auf diesen Systemen.

3. Klassifizierung und Kennzeichnung von Informationen

3.1 Klassifizierung

Um den Schutz und die Kontrolle über den Zugang zu unseren Informationen sicherzustellen, müssen alle Informationen innerhalb unserer Organisation von ihren jeweiligen Eigentümern nach ihrem Inhalt bewertet und klassifiziert werden. Diese Klassifizierung legt das erforderliche Schutzniveau fest und bestimmt, wer auf die Informationen zugreifen darf. Jedes System, das Zugang zu diesen Informationen gewährt, muss die Klassifizierung klar sichtbar anzeigen.

Arten von Informationen:

- Daten in Papierform: Physisch auf Papier gespeicherte Informationen
- Elektronische Daten: In Computersystemen gespeicherte Informationen
- Postalische und elektronische Kommunikation: Informationen, die per Post oder E-Mail ausgetauscht werden
- Elektronische Medien: Informationen auf USB-Laufwerken, Disketten und Bändern.

Personenbezogene Daten umfassen alle Daten, die sich auf identifizierbare Personen beziehen. Unsere Organisation ist gesetzlich verpflichtet, personenbezogene Daten gemäß den nationalen und internationalen Vorschriften zu speichern, zu schützen und zu verwenden. Weitere Informationen zum Umgang mit Privatsphäre und personenbezogenen Daten erhalten Sie von der für den Datenschutz zuständigen Person.

Um die Sicherheit unserer Informationen zu gewährleisten, führt unsere Organisation Verzeichnisse aller wichtigen Informationsbestände. Nähere Informationen hierzu erhalten Sie im Zusammenhang mit der Verwaltung von Informationswerten und -trägern unserer Organisation (siehe ISMS-Handbuch). Wir sind uns der Tatsache bewusst, dass Risiken bestehen, wenn Mitarbeiter, Kunden, Auftragnehmer und andere Dritte auf unsere Informationen zugreifen und mit ihnen arbeiten.

Unsere Organisation verpflichtet sich, die Informationen, die wir besitzen und verarbeiten, durch angemessene Maßnahmen zu schützen, die dem Schutzniveau der Informationen entsprechen. Wir nutzen ein dokumentiertes Klassifizierungsschema, um Informationen genau zu klassifizieren und den nötigen Schutz anzuwenden. Dieses Verfahren beschreibt das Schema und die Kriterien, die zur Bestimmung des Schutzniveaus für jedes Informationsgut verwendet werden.

3.2 Klassifizierungsschema

Unsere Organisation hat folgendes Klassifizierungsschema festgelegt, um Informationen zu schützen. Alle Informationen lassen sich in eine von vier Kategorien einteilen. Das Schema bestimmt, wie Sie Dokumente handhaben, veröffentlichen, bewegen und speichern müssen.

Informationsklassen:

- **Öffentlich (Stufe 0):** Informationen, die jeder sehen darf. Z.B. Jahresberichte, die auf der Website veröffentlicht werden.
- **Intern (Stufe 1):** Informationen, die nur innerhalb der Organisation genutzt werden. Z.B. Interne E-Mails und Mitteilungen.
- **Vertraulich (Stufe 2):** Wichtige Informationen, die nur bestimmte Personen sehen dürfen. Z.B. Kundenlisten und Geschäftspläne.
- **Streng vertraulich (Stufe 3):** Sehr wichtige Informationen, die nur wenige Personen sehen dürfen. Z.B. Unveröffentlichte Finanzergebnisse und vertrauliche Entwicklungsprojekte.

Zuständigkeit für die Klassifizierung von Informationen

Jede Abteilung oder jeder Mitarbeiter, der Informationen erstellt oder verwaltet, ist dafür verantwortlich, diese zu klassifizieren und dadurch festzulegen, wie Informationen zu handhaben, zu veröffentlichen, zu bewegen und zu speichern und am Ende des Lebenszyklus zu vernichten sind. Informationsinhaber müssen die Sensibilität der Informationen bewerten und die geeignete Klassifizierung anwenden. Zudem haben folgende Rollen weitere Verantwortlichkeiten:

- Abteilungsleiter und Vorgesetzte sind dafür verantwortlich, dass alle Mitarbeiter in ihrer Abteilung die Klassifizierungsrichtlinien kennen und anwenden. Sie müssen sicherstellen, dass die Klassifizierung korrekt durchgeführt wird und gegebenenfalls Unterstützung bieten.
- Der Datenschutzbeauftragte überprüft die Einhaltung der Datenschutzrichtlinien und unterstützt bei der Klassifizierung personenbezogener Daten. Er berät bei Fragen zur Datenschutzgesetzgebung und sorgt dafür, dass die Klassifizierungsrichtlinien den gesetzlichen Anforderungen entsprechen.
- Der Sicherheitsbeauftragte sorgt für die Implementierung und Überwachung der physischen und digitalen Sicherheitsmaßnahmen, die den Klassifizierungsstufen entsprechen. Er führt regelmäßige Audits durch, um die Einhaltung der Sicherheitsrichtlinien sicherzustellen.

3.3 Kennzeichnung von klassifizierten Informationen

Unsere Organisation legt fest, dass eine explizite Kennzeichnung von Informationen der Stufen 0 (öffentlich) und & 1 (intern) grundsätzlich nicht gekennzeichnet werden müssen. Somit sind alle ungekennzeichneten Informationen der Organisation als „intern“ zu klassifizieren. Eine Kennzeichnung öffentlicher Informationen der Organisation ist nicht erforderlich, weil diese Informationen aufgrund ihres Charakters, ihres Inhalts und ihrer Präsentationsorte als öffentlich zu identifizieren sind.

Kennzeichnen sie vertrauliche (Stufe 2) und streng vertrauliche (Stufe 3) Informationen klar mit ihrer jeweiligen Klassifikationsstufe, um Missverständnisse oder missbräuchliche Nutzung zu vermeiden. Als Informationseigentümer sind Sie dafür zuständig regelmäßig zu überprüfen, ob die Kennzeichnungen noch aktuell sind, und passen Sie sie gegebenenfalls an.

3.4 Verfahren zur Umsetzung der Klassifizierung und Kennzeichnung

1. **Identifizierung der Informationen:**
    a. Bestimmen Sie die Art und den Inhalt der Informationen.
    b. Überlegen Sie, welche Informationen in Ihrem Arbeitsbereich vorhanden sind.
2. **Bewertung der Informationen:**
    a. Überprüfen Sie, ob die Informationen gesetzliche Anforderungen erfüllen müssen.
    b. Schätzen Sie den Wert der Informationen für die Organisation ein.
    c. Berücksichtigen Sie die Bedeutung der Informationen für die Organisation.
    d. Bewerten Sie das Risiko, wenn die Informationen unbefugt offengelegt oder verändert werden.
3. **Zuweisung der Klassifizierung:**
    a. Verwenden Sie die Kriterien zur Einstufung in Stufe 0 (Öffentlich), Stufe 1 (Intern), Stufe 2 (Vertraulich) oder Stufe 3 (Streng vertraulich).
    b. Dokumentieren Sie die Klassifizierung entsprechend den folgenden Kennzeichnungsanweisungen auf dem Dokument oder im System.
4. **Zugriffskontrolle:**
    a. Überprüfen Sie, wer Zugriff auf die klassifizierten Informationen benötigt.
    b. Stellen Sie sicher, dass nur berechtigte Personen Zugang erhalten.
    c. Befolgen Sie hierbei bestehende Zugangskontrollrichtlinien, um den Zugriff zu verwalten.
5. **Kennzeichnung der Informationen:**
    a. Bringen Sie geeignete Schutzkennzeichnungen an.
    b. Stellen Sie sicher, dass die Klassifizierung klar erkennbar ist.

Beispiele für Kennzeichnungen:

Elektronische Dokumente:

- Verwenden Sie Dateinamen, die die Klassifizierung enthalten. Beispiel: "Bericht_Q2_2024_Vertraulich.docx".
- Nutzen Sie Metadatenfelder innerhalb des Dokumentes oder des Dateisystems, um die Klassifizierung zu speichern.

E-Mails:

- Geben Sie die Klassifizierung im Betreff der E-Mail an. Beispiel: [Vertraulich] Meeting-Protokoll".
- Fügen Sie die Klassifizierung in die Kopfzeile der E-Mail-Nachricht ein.
- Sorgen Sie ebenfalls für eine Kennzeichnung der Herkunft Ihrer E-Mail, sobald diese die Organisation verlässt, und geben Sie klare Anweisungen über den vertraulichen Gebrauch Ihrer Informationen

Datenträger und Speichermedien:

- Bringen Sie physische Etiketten an USB-Laufwerken, CDs, DVDs und anderen Speichermedien an.
- Verwenden Sie beschriftbare Aufkleber oder direkte Beschriftungen auf dem Medium.

Physische Dokumente (z.B. Papier):

- Verwenden Sie gut sichtbare Textmarkierungen, Stempel, Aufkleber oder handschriftliche Vermerke, um die Klassifizierung auf jedem Dokument der Stufen 2 & 3 anzugeben.
- Platzieren Sie die Kennzeichnung oben auf der ersten Seite des Dokuments und, falls möglich, auf jeder weiteren Seite.

Zusätzliche Hinweise:

- Verwenden Sie einheitliche Kennzeichnungen für alle Dokumente.
- Bei Unsicherheit über die Klassifizierung wenden Sie sich an Ihren Vorgesetzten oder die IT-Abteilung.
- Beachten Sie stets die geltenden Datenschutz- und Sicherheitsrichtlinien.

4 Übertragung von Werten

4.1 Informationsübertragung

Informationen aus unserer Organisation können sowohl intern, aber auch extern über folgende elektronische Kommunikationswege ausgetauscht werden: E-Mail, Downloads von Dateien aus dem Internet, Übertragung von Daten über weitere Cloud-basierte Kommunikationssysteme, Telefone, Faxgeräte, der Versand von SMS-Textnachrichten, tragbare Medien, sowie Foren und soziale Netzwerke.

Für die Kommunikation zu dienstlichen Zwecken sind stets die von der Organisation zur Verfügung gestellten elektronischen Nachrichtendienste zu verwenden. Persönliche Konten dürfen für diesen Zweck nicht verwendet werden.

Behandeln Sie alle Nachrichten der Organisation als offizielle Mitteilungen und kennzeichnen Sie diese mit entsprechenden Signaturangaben und – sofern erforderlich -mit entsprechenden Vertraulichkeitsanweisungen.

4.2 Externe Parteien

bevor Sie sensible Informationen oder Software auf elektronischem, physischem oder mündlichem Wege mit externen Parteien austauschen, ist es erforderlich, eine entsprechende schriftliche Vereinbarung vorzubereiten und zu unterzeichnen. Diese Vereinbarung sichert unser Unternehmen ab und stellt sicher, dass beide Parteien die gleichen Sicherheitsstandards einhalten. Hier sind die wichtigen Punkte, die jede Vereinbarung abdecken muss:

- **Identifizierung der anderen Partei:** Stellen Sie sicher, dass die Identität der externen Partei eindeutig festgelegt ist.
- **Zugangsberechtigungen:** Klären Sie, welche Informationen geteilt werden dürfen und wer darauf Zugriff hat.
- **Nichtabstreitbarkeit:** Sichern Sie Maßnahmen ab, die die Authentizität der geteilten Daten gewährleisten.
- **Technische Standards:** Vereinbaren Sie die technischen Standards, die für die Datenübertragung verwendet werden.
- **Umgang mit Vorfällen:** Legen Sie Verfahren fest, die bei Sicherheitsvorfällen oder Datenverlust zu befolgen sind.
- **Umgang mit „vertraulich“ und „streng vertraulich“ klassifizierten Informationen:** Definieren Sie, wie sensible Informationen zu kennzeichnen und zu behandeln sind.
- **Urheberrecht:** Stellen Sie sicher, dass Urheberrechte und andere geistige Eigentumsrechte respektiert werden.

Diese Vereinbarungen müssen in Übereinstimmung mit unserer[Ergänzen Sie die entsprechende Richtlinie für Lieferantenmanagement] erstellt werden. Die Verträge können entweder in Papierform oder elektronisch, z.B. durch Zustimmung zu Allgemeinen Geschäftsbedingungen, ausgeführt werden.

Bitte nehmen Sie diese Verantwortung ernst und stellen Sie sicher, dass alle erforderlichen Vereinbarungen vor dem Austausch von Informationen oder Software vollständig unterzeichnet sind. Bei Fragen oder Unsicherheiten wenden Sie sich bitte an die Rechtsabteilung oder Ihren Vorgesetzten.

4.3 Surfen im Internet

um sicherzustellen, dass unser Arbeitsplatz sicher und produktiv bleibt, sowie eine unangemessene Übertragung von Informationen im Internet vermieden wird, befolgen Sie bitte die folgenden Richtlinien zum Surfen im Internet:

1. **Arbeitsbezogene Nutzung:**

a. Nutzen Sie das Internet während der Arbeitszeit hauptsächlich für arbeitsbezogene Aufgaben.

b. Vermeiden Sie das Besuchen von Webseiten, die nichts mit Ihrer Arbeit zu tun haben.

2. **Sichere Webseiten:**

   a. Besuchen Sie nur vertrauenswürdige und sichere Webseiten.

   b. Laden Sie keine Software oder Dateien aus unbekannten Quellen herunter.

   c. Bedenken Sie, dass auch frei im Internet verfügbare Anwendungen, Software, Daten, Bilder etc. dem Urheberrecht unterliegen und entsprechende Lizenzvorgaben eingehalten werden müssen.

3. **Vertrauliche Informationen:**

   a. Geben Sie keine vertraulichen Informationen auf unsicheren Webseiten ein.

   b. Achten Sie darauf, dass Sie sich nur auf sicheren (https) Webseiten anmelden.

4. **Vermeiden von Risiken:**

   a. Öffnen Sie keine verdächtigen Links oder E-Mail-Anhänge.

   b. Seien Sie vorsichtig bei der Eingabe von persönlichen oder finanziellen Informationen.

Seien Sie sich bewusst, dass viele Verstöße gegen die Informationssicherheit durch "Phishing" erfolgen, d. h. durch bösartige Anhänge oder Links zu Websites, die darauf abzielen, Informationen zu stehlen, in E-Mails oder anderen Nachrichten. Wenn Sie eine Nachricht oder verdächtige Aktivitäten erkennen, melden Sie diese sofort über die im Verlauf dieses Handbuchs definierten Meldekanäle ohne Anhänge zu öffnen oder auf Links zu klicken.

4.4 Cloud Computing

Cloud-Dienste spielen eine wichtige Rolle bei der Ermöglichung reaktionsschneller und flexibler Geschäftsprozesse in unserer Organisation. Während der Nutzung von Cloud-Diensten werden diverse Informationswerte an externe Organisationen übertragen. Diese Übertragung muss kontrolliert erfolgen. Daher muss sichergestellt werden, dass diese Dienste die geschäftlichen, sicherheitstechnischen und rechtlichen Anforderungen der Organisation erfüllen. Zur Erfüllung Ihrer Aufgaben dürfen Sie nur Cloud-Dienste nutzen, die von unserer Organisation genehmigt und bereitgestellt werden. Die Speicherung von vertraulichen und streng vertraulichen Informationen in nicht genehmigten Cloud-Diensten ist streng verboten. Bei Fragen zu genehmigten Cloud-Diensten wenden Sie sich an Ihren Vorgesetzen oder den IT-Service.

4.5 Soziale Netzwerke

Soziale Medien werden von unserer Organisation ausgiebig genutzt, um direkt mit Kunden zu kommunizieren, Produkte und Dienstleistungen zu unterstützen und Feedback über die Wahrnehmung der Organisation zu sammeln. Wenn es zu Ihren Aufgaben gehört, können Sie befugt sein, die Social-Media-Konten des Unternehmens zu nutzen und die Organisation in der Öffentlichkeit zu vertreten.

Toleranz und Respekt sind für uns elementar. Das gilt auch für den Schutz der Privatsphäre unserer Teammitglieder. Wir dulden keine hetzerischen, beleidigenden oder diskriminierenden Beiträge in sozialen Medien. Inakzeptabel sind unter anderem Beiträge, die verfassungsfeindliche Inhalte widerspiegeln, die Würde anderer Nutzer verletzen, den Betriebsfrieden gefährden, unseren Ruf und den Ruf unserer Teammitglieder in Misskredit bringen oder das Verhältnis zu wichtigen Stakeholdern belasten.

5. Aufbewahrung, Rückgabe & Löschung von Informationswerten

5.1 Aufbewahrung von Informationswerten und -trägern

Um unsere Informationen vertraulich, sicher und organisiert aufzubewahren, befolgen Sie bitte die folgenden Richtlinien:

1. **Physische Dokumente:**

   a. Bewahren Sie alle wichtigen bzw. vertraulichen Dokumente in abschließbaren Schränken oder sicheren Bereichen auf.

   b. Stellen Sie sicher, dass nur berechtigte Personen Zugang zu diesen Dokumenten haben.

c. Löschen Sie Notizen auf Whiteboards und Flipcharts z.B. in Büros und Konferenzräumen unmittelbar im Anschluss an Ihre Besprechung.

2. **Elektronische Daten:**

   a. [Empfehlung: Organisationen, die ihre Systemlandschaft ausschließlich über Cloud-Dienste betreiben, haben die empfohlene Möglichkeit, allen Mitarbeitern das Speichern von Daten auf lokalen Speichermedien zu untersagen. Eine solche „No-Local-Files“ Regelung verlangt von jedem Mitarbeiter die Speicherung von Daten ausschließlich in der Cloud. Sie schützt Daten besser vor Verlust und erhöht die Verfügbarkeit durch Kollegen innerhalb des Teams. In solchen Fällen lautet die Anweisung: „Speichern sie keine Daten auf lokalen Speichermedien, wie Laptops, mobilen Speichern, USB-Sticks etc., sondern nur auf sicheren, von der IT-Abteilung genehmigten Servern oder Cloud-Diensten“]
   Speichern Sie elektronische Daten auf sicheren, von der IT-Abteilung genehmigten Speichermedien, Servern oder Cloud-Diensten.

   b. Verwenden Sie starke Passwörter und ändern Sie diese regelmäßig.

3. **Datenträger und Geräte mit gespeicherten Informationen:**

   a. Bewahren Sie Geräte mit Speichereinheiten, USB-Laufwerke, CDs und andere Speichermedien sicher auf und stellen Sie sicher, dass sie entsprechend den Verschlüsselungsrichtlinien verschlüsselt sind.

   b. Kennzeichnen Sie die Datenträger entsprechend ihrer Klassifizierung (z. B. vertraulich, streng vertraulich).

4. **Zugangsbeschränkungen:**

   a. Gewähren Sie nur denjenigen Personen Zugang zu Informationen, die diesen für ihre Arbeit benötigen.

   b. Überprüfen Sie regelmäßig die Zugangsberechtigungen und passen Sie diese bei Bedarf an.

5.2 Rückgabe von Informationswerten und -trägern

Wenn Sie unsere Organisation verlassen oder durch einen Wechsel Ihrer Aufgabenbereiche übertragene Informationswerte und Geräte auf denen diese gespeichert sind, für Ihre Arbeit nicht mehr benötigen, müssen diese unmittelbar zurück gegeben werden. Beachten Sie dabei bitte folgende Richtlinien:

1. **Vorbereitung der Rückgabe:**

   a. Überprüfen Sie alle Informationen und Materialien, die Sie zurückgeben möchten, auf Vollständigkeit und Aktualität.

   b. Entfernen Sie persönliche Daten oder nicht relevante Informationen von den Materialien, falls vorhanden.

   c. Löschen Sie keine Firmendaten oder Anwendungen eigenständig. Informieren Sie die IT-Abteilung, damit sie die Daten sachgemäß sichern oder entfernen kann.

2. **Termin und Ort der Rückgabe:**

   a. Vereinbaren Sie einen spezifischen Termin und Ort für die Rückgabe mit Ihrem Vorgesetzten oder der zuständigen Abteilung.

   b. Halten Sie den vereinbarten Termin ein, um eine ordnungsgemäße und effiziente Rückgabe zu gewährleisten.

3. **Dokumentation der Rückgabe:**

   a. Führen Sie eine detaillierte Liste aller zurückgegebenen Artikel.

   b. Lassen Sie die Rückgabe von einer zuständigen Person quittieren, um eine Bestätigung der erfolgten Rückgabe zu haben.

5.3 Löschung von Informationen

Tragen Sie dazu bei, dass eine unnötige Offenlegung sensibler Daten gegen gesetzliche, behördliche regulative oder vertragliche Anforderungen vermieden wird, indem Sie:

Informationen, die in Informationssystemen, Cloud-Diensten, Geräten oder auf anderen Speichermedien gespeichert sind, gelöscht werden, wenn sie nicht mehr benötigt werden.

- Als Informationseigentümer Ihre Kollegen darüber informieren, dass die von Ihnen verantwortete Informationen nicht mehr benötigt werden und gelöscht werden sollen.

- Den Anweisungen von zentralen Instanzen, wie z.B. dem IT-Service folgeleisten und Löschungsanweisungen befolgen.

5.4 Entsorgung von Geräten mit Datenspeichern

Geräte mit Datenspeichern können auch über ihre Lebenszeit hinaus Informationen ungewollt offenlegen. Daher müssen Sie zum Ende deren Lebenszeit fachgerecht entsorgt werden. Unsere Organisation hat festgelegt, dass ausnahmslos alle Geräte, auf denen sich sensible Informationen der Organisation befinden können, über den zentralen IT-Service entsorgt werden müssen. Orientieren Sie sich bei der Übergabe der zu entsorgenden Geräte and den zuvor genannten Rückgaberegeln von Informationswerten & -trägern.

[Hinweis: Die hier behandelte Richtlinie steht in Bezug zur Physischen Sicherheit Ihrer Organisation. Bitte gleichen Sie eventuelle Ergänzungen/Anpassungen auch mit den Richtlinien in Ihrem Handbuch für physische Sicherheit (DataGuard Policy-Vorlage ST10) ab.]

6. Schutz von geistigem Eigentum

Geistiges Eigentum – ungeachtet ob fremdes oder solches von unserer Organisation – muss für den Erfolg und die Wettbewerbsfähigkeit unserer Organisation geschützt werden. Daher bitten wir Sie, die folgenden Richtlinien sorgfältig zu befolgen:

1. **Eigenes geistiges Eigentum:**
    a. **Wahren Sie Vertraulichkeit:** Diskutieren Sie vertrauliche Projekte und Informationen nur mit autorisierten Personen innerhalb der Organisation. Verwenden Sie bei der Kommunikation über sensible Inhalte stets gesicherte und genehmigte Plattformen.
    b. **Dokumentation und Kennzeichnung:** Kennzeichnen Sie alle Dokumente, die geistiges Eigentum enthalten, deutlich als vertraulich. Halten Sie alle Erstellungsdaten und Änderungen an geistigen Eigentumswerten akribisch fest.
    c. **Nutzung von Technologien:** Speichern Sie alle digitalen Informationen auf sicheren Servern oder in der Cloud unter Einhaltung unserer IT-Sicherheitsrichtlinien. Organisieren Sie die Zugangsrechte für geistigen Eigentum strikt nach dem „Need-to-Know-Prinzip“. Entfernen Sie persönliche Daten oder nicht relevante Informationen von den Materialien, falls vorhanden.
    d. **Melden von Verdachtsfällen:** Melden Sie sofort jegliche verdächtigen Aktivitäten oder mögliche Sicherheitsverletzungen an die zuständige Abteilung. Arbeiten Sie bei Untersuchungen zu Verstößen gegen das geistige Eigentum aktiv mit.
2. **Fremdes geistiges Eigentum:**
    a. **Genehmigung und Lizenzen:** Nutzen Sie keine urheberrechtlich geschützten Materialien ohne die erforderliche Genehmigung oder Lizenz.
    b. **Korrekte Nutzung und Zitierung:** Stellen Sie sicher, dass alle verwendeten externen Inhalte ausschließlich nach den aktuellen Lizenzvereinbarungen korrekt genutzt und zitiert werden und Quellenangaben klar erkennbar sind.
    c. **Erfassung von kostenpflichtigen Lizenzen:** Führen Sie Vertragsbedingungen wie z.B. Lizenzlaufzeiten, Kündigungsfristen, Preise bzw. Preisänderungen in Ihrem Assetverzeichnis bzw. informieren Sie ggf. die für die Verwaltung, Beschaffung oder kaufmännische Abwicklung zuständigen Bereiche darüber.
    d. **Meldung von Unsicherheiten:** Melden Sie jegliche Unsicherheiten oder mögliche Verstöße gegen die Richtlinien sofort an Ihre Vorgesetzten oder die Rechtsabteilung.

7. Umgang mit künstlicher Intelligenz

Die Integration von Künstlicher Intelligenz (KI) in unsere Arbeitsprozesse bietet viele Vorteile, bringt jedoch auch spezifische Verantwortlichkeiten mit sich, besonders im Hinblick auf Informationssicherheit, Vertraulichkeit und den Schutz von Urheberrechten. Bitte beachten Sie die folgenden Richtlinien:

Datenschutz und Vertraulichkeit:

Stellen Sie sicher, dass alle durch KI-Systeme verarbeiteten oder generierten Daten gemäß unseren Datenschutzrichtlinien und den geltenden Datenschutzgesetzen behandelt werden.

Nutzen Sie KI-Tools nur in einer Weise, die die Vertraulichkeit von Unternehmensdaten wahrt. Achten Sie darauf, dass sensible Informationen nicht ungeschützt oder unautorisiert preisgegeben werden.

Urheberrechtsschutz:

Achten Sie darauf, keine urheberrechtlich geschützten Daten ohne entsprechende Lizenz oder Erlaubnis in KI-Systeme einzuspeisen.

Informieren Sie sich über die Urheberrechte von Daten und Algorithmen, die in KI-Tools verwendet werden, um Verletzungen zu vermeiden.

Sicherer Umgang mit Daten:

Verwenden Sie nur autorisierte und sichere Datenquellen, wenn Sie KI-Systeme speisen oder trainieren.

Überprüfen Sie regelmäßig die Zugriffsrechte auf KI-Anwendungen, um sicherzustellen, dass nur berechtigte Personen Zugang haben.

Ethische Nutzung:

Verwenden Sie KI-Technologien ethisch verantwortungsbewusst. Vermeiden Sie den Einsatz von KI zur Überwachung oder zur Bewertung von Mitarbeitern ohne deren Wissen und Zustimmung.

Seien Sie sich der Auswirkungen bewusst, die der Einsatz von KI auf die Privatsphäre und die Rechte von Einzelpersonen haben kann.

Validierung und Überwachung:

Überprüfen und validieren Sie regelmäßig die Ausgaben der KI-Systeme, um sicherzustellen, dass diese korrekt und frei von Voreingenommenheit sind.

Melden Sie Anomalien oder potenzielle Sicherheitsrisiken sofort an das IT-Sicherheitsteam.

Schulung und Bewusstsein:

Nehmen Sie an Schulungen teil, um ein besseres Verständnis für die Funktionen, Möglichkeiten und Risiken der KI-Technologie zu entwickeln.

Bleiben Sie informiert über neue Entwicklungen im Bereich KI und deren Implikationen für Sicherheit und Compliance.

Durch die Einhaltung dieser Richtlinien tragen Sie dazu bei, das Potenzial von KI sicher und effektiv zu nutzen, während Sie gleichzeitig unsere Daten schützen und rechtliche sowie ethische Standards wahren.

8. Identitäts- & Kennwortnutzung

[Hinweis: Die in Kap. 8 behandelten Richtlinien stehen in Bezug zum Identitäts- und Zugriffsverwaltung Ihrer Organisation. Bitte gleichen Sie eventuelle Ergänzungen/Anpassungen auch mit den Richtlinien in Ihrem Handbuch zur Sicherheit in Indentitäts- und Zugriffsverwaltung (DataGuard Policy-Vorlage ST9) ab.]

8.1 Nutzung von Identitäten bzw. Kennwörtern

Um die Sicherheit unserer Informationen, Werte und Systeme zu gewährleisten, bitten wir Sie, die folgenden Richtlinien zur Nutzung von Identitäten und Kennworten strikt zu befolgen:

Geheimhaltung von Kennworten:

Geben Sie Ihre Kennworte niemals an andere Personen weiter, einschließlich Geschäftsführung oder Systemadministratoren. Jedoch müssen gesetzliche Pflichten auch hier nach Rücksprache mit der Unternehmensleitung erfüllt werden.

Schreiben Sie Ihre Kennworte nicht auf, es sei denn, es wurde eine sichere Methode durch Ihre Vorgesetzten genehmigt.

Erstellung und Verbreitung von Kennworten:

Ändern Sie Ihr Kennwort sofort bei der erstmaligen Anmeldung an einem neuen System.

Verbreiten Sie selbst erstellte Kennworte nicht mündlich, schriftlich oder in elektronischer Form.

Anforderungen an sichere Kennworte:

Wählen Sie Kennworte mit mindestens 16 Zeichen, die mindestens eine Ziffer, einen Großbuchstaben, einen Kleinbuchstaben und ein Sonderzeichen enthalten.

Vermeiden Sie Wörter, die in Wörterbüchern stehen, Dialektwörter oder umgangssprachliche Ausdrücke, sowie persönliche Daten wie Geburtsdaten oder Namen.

Verwenden Sie die letzten drei Kennworte nicht wieder.

Regelmäßige Änderung von Kennworten:

Ändern Sie Ihre Kennworte alle drei Monate.

Speichern Sie Kennworte nicht für die automatische Anmeldung in Systemen wie Makros oder Browsern.

Verwenden Sie keine privaten Kennworte für Geschäftszwecke.

Ausnahmefälle & Vorfallmeldung:

Sollten bestimmte Regeln aufgrund von Systembeschränkungen nicht anwendbar sein, wenden Sie die stärksten verfügbaren Sicherheitspraktiken an.

Melden Sie umgehend einen Sicherheitsvorfall, wenn Sie den Verdacht haben, dass Ihr Kennwort oder das System kompromittiert wurde.

8.2 Antragverfahren von Zugangsrechten

Ein Antragprozess zur Vergabe von Zugangsrechten auf Dateien stellt sicher, dass nur autorisierte Mitarbeiter Zugriff auf sensible Informationen haben. In unserer Organisation erfolgt der Antragprozess wie folgt [Bitte passen Sie den folgenden Antragprozess an Ihre Organisation an]:

Bedarfsanalys:

Identifizieren Sie, welche Dateien oder Verzeichnisse sie für Ihre Arbeit benötigen.

Besprechen sie dies ggf. mit Ihrem Vorgesetzten, um den tatsächlichen Bedarf zu prüfen.

Antragstellung:

Stellen Sie einen formalen Antrag, indem Sie …[Bitte beschreiben Sie den in Ihrer Organisation eingerichteten Antragprozess].

Genehmigung:

Ihr Vorgesetzter [bzw. Ihre zuständige Instanz] überprüft den Antrag, bewertet den Bedarf und genehmigt oder lehnt den Antrag ab.

Eine Genehmigung erfolgt unter Berücksichtigung der jeweiligen Klassifizierung der freizugebenden Informationen bzw. unserer Sicherheitsrichtlinien, die durch die Eigentümer der Informationen definiert wurden.

Vergabe von Zugangsrechten und entsprechende Dokumentation:

Nach der formalen Genehmigung wird der Antrag an die IT-Abteilung weitergeleitet, die ebenfalls den Antrag auf technische Machbarkeit und Einhaltung der Sicherheitsstandards überprüft.

Die IT-Abteilung richtet die erforderlichen Zugangsrechte ein.

Der Mitarbeiter wird über die erfolgreichen Änderungen und den Zugang informiert.

Der gesamte Prozess, einschließlich Genehmigungen und Zugriffsänderungen, wird dokumentiert.

Diese Dokumentation dient zur Nachverfolgbarkeit und zur Einhaltung von Auditrichtlinien.

Diese Richtlinien sind entscheidend, um unsere Daten und Systeme zu schützen. Wir zählen auf Ihre Mitarbeit und Ihr Engagement, um unsere IT-Sicherheit zu gewährleisten.

9. Arbeiten innerhalb und außerhalb der Geschäftsräume

[Hinweis: Die in Kap. 9 behandelten Richtlinien stehen in Bezug zur physischen Sicherheit Ihrer Organisation. Bitte gleichen Sie eventuelle Ergänzungen/Anpassungen auch mit den Richtlinien in Ihrem Handbuch für physische Sicherheit (DataGuard Policy-Vorlage ST10) ab.]

9.1 Sichern von Büros, Räumen und Einrichtungen

um die Sicherheit unserer Geschäftsräume zu gewährleisten, bitten wir Sie, die folgenden einfachen Anweisungen zu beachten:

1. **Zugangskontrolle:**
    a. Tragen Sie stets Ihren Mitarbeiterausweis sichtbar, und verwenden Sie ihn, um durch gesicherte Türen zu gelangen. [sofern anwendbar]
    b. Lassen Sie keine unbekannten Personen ohne Begleitung in unsere Räumlichkeiten.
    c. Alle Besucher müssen angemeldet und registriert werden. Bei längeren Aufenthalten von mehr als einem Tag ist es zudem erforderlich, dass Besucher in die örtlichen Sicherheitsmaßnahmen des Standortes eingewiesen werden.
2. **Fenster und Türen:**
    a. Schließen Sie alle Fenster, wenn Sie das Gebäude am Abend verlassen, um unbefugten Zugang und Wettereinflüsse zu vermeiden.
    b. Achten Sie darauf, dass sensible Informationen nicht von gegenüberliegenden Gebäuden oder der Straße aus einzusehen sind.
    c. Halten Sie Türen, besonders Außentüren, immer geschlossen. Öffnen Sie sie nicht für Unbekannte oder halten Sie sie nicht unnötig offen.
3. **Melden von Sicherheitsrisiken:**
    a. Melden Sie sofort alle Sicherheitsrisiken oder defekte Schließmechanismen an Ihre Vorgesetzten oder die Haustechnik.

Diese Maßnahmen helfen uns, unsere Arbeitsplätze sicher zu halten und schützen sowohl unsere persönliche Sicherheit als auch die Sicherheit unserer Informationen und Vermögenswerte.

9.2 Schutz von Endpunktgeräten

Alle im Zusammenhang mit Ihrer Arbeit genutzten Datenverarbeitungsgeräte, wie Rechner, Notebooks, Drucker, Smartphones und Tablets müssen durch die folgenden Maßnahmen geschützt werden:

1. **Antivirus- und Anti-Malware-Software:**
    a. Installation und regelmäßige Aktualisierung von Antivirus- und Anti-Malware-Software, um Geräte vor schädlichen Programmen zu schützen. Diese Software sollte in Echtzeit Bedrohungen erkennen und entfernen können.
2. **Verschlüsselung:**
    a. Vollständige Festplattenverschlüsselung oder spezifische Dateiverschlüsselung muss angewendet werden, um sicherzustellen, dass Informationen selbst bei Verlust oder Diebstahl des Geräts nicht ohne Weiteres gelesen werden können.
3. **Zugangskontrollen:**
    a. Richten Sie starke Authentifizierungsmechanismen wie komplexe Passwörter, biometrische Authentifizierung (Fingerabdruck, Gesichtserkennung) oder Zwei-Faktor-Authentifizierung (2FA) ein, um den unbefugten Zugriff auf das Gerät zu verhindern.
4. **Regelmäßige Software-Updates:**
    a. Stellen Sie sicher, dass das Betriebssystem und alle Anwendungen regelmäßig auf die neueste Version aktualisiert werden. Updates enthalten oft Sicherheits-Patches, die bekannte Schwachstellen beheben.

Bei Geräten, die Ihnen von unserer Organisation durch die IT-Abteilung zur Verfügung gestellt werden, liegt die Umsetzung dieser Anforderungen in der Verantwortung der Fachabteilung. In diesem Fall stellen Sie bitte sicher, dass die Kollegen Gelegenheit für die regelmäßige Umsetzung der Maßnahmen erhält, indem der Zugriff auf die Geräte ermöglicht wird.

Diese Maßnahmen tragen dazu bei, die Sicherheit von Endpunktgeräten zu gewährleisten und sensible Unternehmensinformationen zu schützen.

9.3 Nutzung eigener Endpunktgeräte (BYOD)

Die Nutzung von persönliche bzw. privaten Endpunktgeräten ist innerhalb von unsere Organisation streng reglementiert und muss mit den verantwortlichen Stellen abgestimmt werden.

Sollten Sie in Ihrem individuellen Fall eine Nutzung Ihrer eigenen elektronischen Geräte für geschäftliche Zwecke anstreben, wenden Sie sich bitte an Ihre Vorgesetzen, um dies abzustimmen. In diesem Fall wird mit Ihnen eine zusätzliche Arbeitsvereinbarung getroffen, der eine eigene BYOD-Richtlinie zugrunde liegt. Die im vorgenannten Punkt genannten Schutzmaßnahmen sind auch für private Endpunktgeräte bindend. Für weitere Fragen steht Ihnen Ihr Vorgesetzter und die Ihr IT-Service zur Verfügung.

9.4 Sicheres Aufstellen von Geräten

Zur Sicherstellung der Verfügbarkeit von Informationssystemen, aber auch zum Schutz und zur Vermeidung von Unfällen befolgen Sie bitte folgende Anweisungen:

- **Richtige Platzierung:** Stellen Sie alle Geräte, insbesondere schwerere wie Drucker oder Computermonitore, auf stabile, ebene Flächen, die speziell dafür vorgesehen sind. Vermeiden Sie es, schwere Geräte auf instabilen oder leicht zu bewegenden Möbelstücken zu platzieren.
- **Kabelmanagement:** Ordnen und sichern Sie alle Kabel und Leitungen, um Stolperfallen zu vermeiden. Verwenden Sie Kabelbinder oder Kabelkanäle, um Kabel geordnet und nahe an Wänden oder unter Schreibtischen zu führen, damit sie nicht lose herumliegen.
- **Belüftung:** Achten Sie darauf, dass alle Lüftungsöffnungen von Computern, Druckern und anderen elektronischen Geräten frei sind, um eine Überhitzung zu verhindern. Stellen Sie Geräte nicht direkt gegen Wände oder in enge Ecken, wo die Luftzirkulation eingeschränkt ist.
- **Zugang für Wartung:** Stellen Sie sicher, dass rund um die Geräte genügend Raum vorhanden ist, um Wartungsarbeiten oder schnellen Zugriff im Notfall zu ermöglichen. Planen Sie ausreichend Platz für das Öffnen von Türen oder Schubladen an Geräten.
- **Schützen Sie Geräte vor Feuchtigkeit:** Stellen Sie Geräte mit ausreichendem Abstand zu Waschbecken und lebenden Pflanzen auf, sowie zu Fenstern durch die Regen einfallen könnte.

9.5 Aufgeräumte Arbeitsumgebung

Ein aufgeräumter Arbeitsplatz ist nicht nur förderlich für die Produktivität, sondern spielt auch eine entscheidende Rolle im Schutz von sensiblen Informationen. Befolgen Sie bitte folgende Richtlinien, um die Sicherheit von Informationen durch aufgeräumte Arbeitsumgebungen zu gewährleisten:

- Praktizieren Sie die Politik des „Clean Desk“, indem Sie Ihren Arbeitsplatz am Ende jedes Arbeitstages aufräumen. Stellen Sie sicher, dass alle sensiblen Dokumente weggeschlossen und alle elektronischen Geräte gesichert sind.
- Aktivieren Sie biometrische Sicherheitsmaßnahmen oder Passwortschutz auf allen Computern und mobilen Geräten. Stellen Sie sicher, dass diese Sicherheitsmaßnahmen immer aktiviert sind, wenn der Arbeitsplatz verlassen wird.
- Achten Sie beim Teilen Ihres Bildschirms in Video-Calls darauf, dass keine sensiblen Inhalte oder System-Benachrichtigungen sichtbar sind. Nutzen Sie die Funktionen zur Auswahl spezifischer Fenster für die Freigabe, um nur relevante Informationen zu teilen.
- Sorgen Sie dafür, dass Ausdrucke innerhalb Ihres Sichtfeldes passieren oder - wenn möglich - stellen Sie Drucker so ein, dass ein Passwort benötigt wird, bevor Dokumente ausgegeben werden. Dies verhindert, dass vertrauliche Dokumente von Unbefugten eingesehen oder abgeholt werden.
- Nutzen Sie Aktenvernichter für jegliches Papier, dass sensible Informationen enthält (auch Notizen).

9.6 Arbeiten außerhalb der Geschäftsräume

Um die Sicherheit unserer Informationen auch außerhalb der Geschäftsräume (z.B. auf Reisen, im Homeoffice) zu gewährleisten, bitten wir Sie, folgende Richtlinien zu beachten:

- **Vorsicht bei der Nutzung von öffentlichem WLAN:** Vermeiden Sie die Nutzung von öffentlichem WLAN für geschäftliche Aktivitäten, besonders wenn es um den Zugriff auf vertrauliche oder firmeninterne Daten geht. Nutzen Sie stattdessen sichere, persönliche Hotspots.
- **Sichere Netzverbindung:** Verwenden Sie immer sichere, verschlüsselte Verbindungen, wenn Sie online arbeiten.

Nutzen Sie VPN-Zugänge (Virtual Private Network), die von der Firma bereitgestellt werden, um eine sichere Verbindung zum Unternehmensnetzwerk herzustellen. [sofern anwendbar]

- **Schutz vertraulicher Informationen:** Vermeiden Sie auch das temporäre Speichern sensibler oder vertraulicher Informationen auf lokalen Laufwerken oder mobilen Geräten. Nutzen Sie stattdessen ausschließlich gesicherte Cloud-Speicher oder Unternehmensserver.
- **Softwareaktualisierungen oder Patches:** Sorgen Sie dafür, dass trotz Ihrer Abwesenheit auf allen datenverarbeitenden Geräten zeitnah die vorgesehenen Patches und Softwareaktualisierungen ausgeführt werden.
- **Gewährleistung physischer Sicherheit:** Achten Sie darauf, Ihre Arbeitsgeräte wie Laptops, Tablets und Smartphones nie unbeaufsichtigt zu lassen, besonders in öffentlichen oder gemeinschaftlich genutzten Räumen.
- **Diskretion in der Öffentlichkeit:** Führen Sie vertrauliche Gespräche oder Meetings in der Öffentlichkeit nur, wenn es unvermeidlich ist, und achten Sie darauf, dass sie nicht von Unbefugten gehört werden können.
- **Berichterstattung bei Sicherheitsvorfällen:** Melden Sie alle Sicherheitsvorfälle, wie den Verlust oder Diebstahl von Geräten, unverzüglich der IT-Abteilung oder Ihrer Sicherheitskontaktstelle.

[Empfehlung: Ebenso wie bei der Nutzung von privaten Geräten eine separate BYOD-Richtlinie zu empfehlen ist, empfiehlt es sich mit den jeweiligen Mitarbeitern individuell für das „Arbeiten aus dem Homeoffice“ eine separate Richtline zu vereinbaren. Diese sollte auch die Aspekte: Arbeitszeit und Arbeitssicherheit behandeln.]

9.7 Arbeiten in Sicherheitszonen

Sicherheitszonen im Sinne dieser Richtlinien sind Bereiche, in denen besonders sensible Informationswerte zugänglich sind. Serverräume sind zum Beispiel solche Sicherheitszonen. Das Arbeiten in diesen definierten Bereichen unterliegt besonderen Regelungen und ist ausschließlich befugten Personen gestattet. Sofern Sie gezwungen sind, in diesen Sicherheitszonen zu arbeiten, befolgen Sie folgende Richtlinien:

- Betreten Sie entsprechende Sicherheitszonen nur mit entsprechender Genehmigung des Eigentümers der sensiblen Informationswerte.
- Protokollieren Sie alle Ein- und Austritte genau, um eine genaue Übersicht über den Zugang zu diesem Bereich zu haben.
- Berühren oder manipulieren Sie keine Hardware oder Kabel, es sei denn, es ist Teil Ihrer ausdrücklichen Aufgaben.
- Verwenden Sie nur genehmigte Geräte und Software innerhalb der Sicherheitszonen
- Halten Sie Sicherheitszonen sauber und frei von Unordnung, um die Gefahr von Unfällen und Überhitzung dort befindlicher Geräte zu minimieren.
- Vermeiden Sie das Mitbringen von Essen, Getränken und anderen potenziell gefährlichen Gegenständen in Sicherheitszonen.
- Achten Sie darauf, dass die Türen zu Sicherheitszonen immer geschlossen sind, um die Kontrolle über Temperatur und Feuchtigkeit zu gewährleisten.
- Melden Sie jegliche Probleme mit der Klimaanlage oder anderen Umgebungskontrollsystemen sofort.
- Seien Sie mit den Notfallverfahren vertraut, einschließlich der Standorte von Feuerlöschern und Notausgängen.

10. Verhalten bei Ereignissen und Vorfällen

[Hinweis: Die in Kap. 10 behandelten Richtlinien stehen in Bezug zum Vorfallmanagement Ihrer Organisation. Bitte gleichen Sie eventuelle Ergänzungen/Anpassungen auch mit den Richtlinien in Ihrem Handbuch zur Sicherheit in Indentitäts- und Zugriffsverwaltung (DataGuard Policy-Vorlage ST9) ab.]

10.1 Meldung von Ereignissen und Vorfällen

Unsere Organisation ist tagtäglich einer Vielzahl von Risiken ausgesetzt, die die Vertraulichkeit, Verfügbarkeit oder Integrität unserer Informationswerte und Systeme gefährden. Solche Risikoszenarien können aktiv - oder passiv, ohne aktives Zutun ausgelöst werden. Wir nennen solche riskanten Momente „Sicherheits-Ereignisse“.
Oftmals lässt sich die Höhe des Risikos oder gar der bereits entstandene Schaden eines Ereignisses ohne weiteren Kontext und tiefer reichende Informationen nicht bewerten. Dann ist die Bewertung des Ereignisses durch geschulte Kollegen und Experten erforderlich.

Die Sicherheitsstruktur von unserer Organisation verfügt über zahlreiche Überwachungsmaßnahmen. Dennoch sind Ihre Aufmerksamkeit und Meldung von Ereignissen eine unersetzliche Aufgabe, um die Sicherheit in unserer Organisation zu gewährleisten.

Aus diesem Grund fordern wir Sie und unsere Geschäftspartner auf, jegliche Ereignisse, die Sie als ungewöhnlich oder, riskant empfinden, oder die gegen Gesetze, Richtlinien oder Verträge unserer Organisationen verstoßen, zu melden. Es ist es unerlässlich, dass jeder von uns aufmerksam ist und angemessen auf solche Ereignisse reagiert. Ihre aktive Beteiligung ist ein entscheidender Bestandteil unserer Sicherheitskultur. Bitte beachten Sie die folgenden Schritte, wenn Sie ein ungewöhnliches bzw. riskantes Ereignis oder einen Vorfall erkennen:

Sofortige Meldung:

Melden Sie das Ereignis unverzüglich über die im folgenden beschriebenen Meldekanäle und Ihrem Vorgesetzten. Zeitnahe Reaktionen können potenzielle Schäden minimieren.

Dokumentation des Vorfalls:

Dokumentieren Sie alles, was mit dem Vorfall zu tun hat, einschließlich der Zeit des Auftretens, der betroffenen Systeme und der Art des Vorfalls. Diese Informationen sind entscheidend für die Untersuchung und Behebung des Vorfalls.

Keine Eigeninitiative bei der Behebung:

Versuchen Sie nicht, das Problem selbst zu lösen, es sei denn, Sie sind dafür hinreichend geschult. Unsachgemäße Maßnahmen können zusätzliche Probleme verursachen.

Kooperation mit dem Sicherheitsteam:

Folgen Sie den Anweisungen des Sicherheitsteams und unterstützen Sie sie bei der Untersuchung und Behebung des Vorfalls. Ihre Kooperation ist für eine effektive Reaktion entscheidend.

Vertraulichkeit wahren:

Bewahren Sie Stillschweigen über Details des Sicherheitsvorfalls, um keine weiteren Sicherheitsrisiken zu provozieren oder Informationen preiszugeben, die von anderen ausgenutzt werden könnten.

Überprüfung und Nachsorge:

Beteiligen Sie sich an Nachbesprechungen, um aus dem Vorfall zu lernen und zukünftige Vorfälle zu vermeiden. Es ist wichtig, dass alle Mitarbeiter aus solchen Ereignissen lernen.

Aktualisierung Ihrer Sicherheitstrainings:

Nehmen Sie regelmäßig an Sicherheitsschulungen und Übungen teil, um Ihr Wissen über aktuelle Sicherheitsbedrohungen und richtige Reaktionsstrategien zu aktualisieren.

Beispiele für Sicherheitsereignisse:

Phishing-Angriffe: Phishing bezeichnet den Versuch, über gefälschte E-Mails, Webseiten oder Nachrichten an sensible Informationen wie Passwörter oder Kreditkartendaten zu gelangen. Dabei werden oft täuschend echte E-Mails oder Links verwendet, um Nutzer zur Eingabe ihrer Daten auf manipulierten Webseiten zu verleiten.

Ransomware-Angriffe: Bei einem Ransomware-Angriff wird Malware auf einem Computer oder Netzwerk installiert, die Daten verschlüsselt oder Systeme sperrt. Die Angreifer fordern dann ein Lösegeld für die Freigabe der gesperrten Daten oder Systeme.

Datenlecks: Datenlecks treten auf, wenn vertrauliche Informationen durch Fehler oder Sicherheitsl√ºcken unabsichtlich freigegeben oder gestohlen werden. Dies kann durch Konfigurationsfehler, unzureichende Sicherheitsma√ünahmen oder menschliche Fehler verursacht werden.

Insider-Bedrohungen: Insider-Bedrohungen stammen von Personen innerhalb der Organisation, die Zugang zu sensiblen Informationen haben. Diese Personen können absichtlich oder unbeabsichtigt Informationen missbrauchen oder preisgeben, was zu erheblichen Sicherheitsverletzungen führen kann.

DDoS-Angriffe (Distributed Denial of Service): Bei DDoS-Angriffen werden Server oder Netzwerke mit einer Flut von Internetverkehr überlastet, was dazu führt, dass sie nicht mehr erreichbar sind. Dies wird oft durch ein Netzwerk von kompromittierten Computern ausgeführt, die als Botnetz fungieren.

Digitale oder physische Zugangsverletzungen: Nutzung von Zugängen zu Informationswerten durch unberechtigte Personen. Zugänge können in digitaler Form bestehen, wie ein unerlaubter System- oder Datenzugang (z.B. durch gemeinsam genutzte Passwörter), oder in physischer Form, wie unwirksame Sicherheitsmaßnahmen (z.B. eine unerlaubt offenstehende Tür).

Ungeahnt viele weitere Ereignisse: Eine Auflistung an möglichen Ereignissen wird niemals vollständig sein. Durch die sich ständig ändernden Umgebungsbedingungen werden stets neue weitere Ereignisszenarien hinzukommen.

10.2 Meldekanäle

[Die Struktur der Meldekanäle in Ihrer Organisation kann sehr individuell sein und sollte sich an den gewohnten Kommunikationskanälen orientieren. Wählen Sie für die Meldung von Sicherheitsereignissen möglichst einfache und etablierte Verfahren und Kanäle aus. Berücksichtigen Sie auch Meldekanäle, die von Ihren externen Geschäftspartnern erreicht werden können. Auch das Angebot mehrerer verfügbarer Kanäle (z.B. E-Mail, Intranet und Ticket-System) erhöht die Nutzungswahrscheinlichkeit durch Ihre Mitarbeiter.

Bitte beschreiben Sie hier die in Ihrer Organisation eingerichteten Meldekanäle in einfach verständlicher Sprache.]

[Beispiel:]
Die Meldung von Informationssicherheitsvorfällen hängt von der Art und Dringlichkeit der Situation ab. Bei Ereignissen, die bereits eingetreten sind oder wahrscheinlich in Kürze eintreten werden, erfordern dringende Situationen eine sofortige mündliche Mitteilung, entweder persönlich oder über Echtzeit-Kommunikationsmethoden wie Telefon- oder Videokonferenzen. Dies ist notwendig, da andere Kommunikationskanäle möglicherweise nicht genau überwacht werden.

Für die Meldung tatsächlicher oder vermuteter Ereignisse im Bereich der Informationssicherheit können die folgenden aufgeführten Methoden verwendet werden:

- Senden Sie eine E-Mail, rufen Sie an, senden Sie eine SMS, greifen Sie auf ein Webportal zu oder nutzen Sie einen der anderen unterstützten Kanäle, um das Helpdesk unserer Organisation zu kontaktieren:

E-Mail: support@organisation.com

Telefon: +1 234 567 8910

SMS-Text: +44 777 572 1234

Webportal: support.helpdesk.organisation.com

- Im Falle eines physischen Eindringens, z. B. wenn eine unbefugte Person in einem Gebäude vermutet wird, sollte der Sicherheitsdienst des Standorts telefonisch kontaktiert werden, entweder direkt unter der Nummer +1 234 567 8911 oder über den Empfang des entsprechenden Gebäudes unter der Nummer 4444.
- Ein unmittelbarer Manager oder Vorgesetzter kann persönlich oder über interne Kommunikationskanäle wie E-Mail oder Messaging informiert werden.

Erforderliche Informationen bei einer Meldung:

Bei der Meldung eines Informationssicherheits-Ereignisses sollten die folgenden Angaben gemacht werden:

- Name, Funktion, Abteilung, Standort und Kontaktangaben
- Eine Beschreibung der Art des Ereignisses
- Ein Hinweis auf die Dringlichkeit des Ereignisses
- Falls verfügbar, eine Bewertung der möglichen Auswirkungen des Ereignisses

11. Schutz von Hinweisgebern (Whistleblowing)

im Rahmen unseres Engagements für Transparenz und Integrität haben wir die folgenden Richtlinien zum Schutz von Hinweisgebern (Whistleblowing) und ein geschütztes Meldeverfahren festgelegt. Diese Maßnahmen dienen dazu, Personen, die auf Missstände oder rechtswidriges Verhalten innerhalb unserer Organisation hinweisen, zu schützen:

Zweck der Whistleblowing-Richtlinie: Unsere Whistleblowing-Richtlinie soll sicherstellen, dass alle Mitarbeiter die Möglichkeit haben, Bedenken bezüglich unrechtmäßiger oder unethischer Praktiken ohne Angst vor Vergeltung zu melden. Wir erkennen den Wert und die Wichtigkeit an, dass Mitarbeiter Missstände offen ansprechen können.

Zweck der Whistleblowing-Richtlinie: Wir haben ein sicheres und vertrauliches Meldeverfahren eingerichtet, um Ihre Identität zu schützen und sicherzustellen, dass Ihre Bedenken ernst genommen werden. Hier sind die Schritte, die Sie befolgen können: [Bitte ergänzen Sie hier die in Ihrer Organisation eingerichteten Meldeverfahren]

1. **Kontaktieren Sie den Vertrauensbeauftragten [bzw. die in Ihrer Organisation eingesetze Rolle]:** Jeder Mitarbeiter kann sich direkt an unseren Vertrauensbeauftragten wenden, der speziell dafür geschult ist, in solchen Angelegenheiten zu unterstützen.

Vertrauliche Meldung: Sie können Ihre Bedenken anonym über unser Online-Meldesystem oder durch einen vertraulichen Brief an die dafür vorgesehene Adresse äußern.

1. **Follow-Up:** Nachdem Sie Ihre Bedenken geäußert haben, wird unser Compliance-Team eine sorgfältige Untersuchung durchführen. Sie erhalten regelmäßige Updates zum Status Ihrer Meldung.
2. **Schutz vor Vergeltung:** Es ist unser oberstes Ziel, sicherzustellen, dass kein Mitarbeiter, der in gutem Glauben handelt und Missstände meldet, irgendwelche Nachteile oder Vergeltungsmaßnahmen erfährt. Dies schließt Kündigung, Herabstufung, Belästigung oder jede andere Form von Diskriminierung ein.

Wir ermutigen jeden, sich aktiv zu beteiligen und Missstände zu melden, die unseren ethischen Standards oder rechtlichen Verpflichtungen widersprechen. Durch Ihr Engagement helfen Sie uns, ein faires und gerechtes Arbeitsumfeld zu schaffen.

Für weitere Informationen oder bei Fragen zu diesem Verfahren wenden Sie sich bitte an die Personalabteilung oder Ihren direkten Vorgesetzten.

12. Schulung und Disziplinarische Maßnahmen bei Nicht-Einhaltung von Richtlinien

12.1 Schulung

Die kontinuierliche Weiterbildung unserer Belegschaft auch im Bereich der Informationssicherheit ist ein zentraler Bestandteil unseres Unternehmens. Um sicherzustellen, dass wir den hohen Anforderungen unserer Branche gerecht werden und unsere Position am Markt stärken, ist die aktive Teilnahme an unseren Schulungsangeboten unerlässlich. Wir bitten Sie daher um Beachtung der folgenden Richtlinien:

1. **Verpflichtung zur Teilnahme:** Alle Mitarbeiter sind verpflichtet, an den von der Unternehmensleitung festgelegten Schulungen teilzunehmen. Diese Schulungen sind darauf ausgelegt, Ihre Fähigkeiten zu erweitern und auf dem neuesten Stand zu halten.
2. **Schulungsangebote:** Wir bieten eine Vielzahl von Schulungsprogrammen an, die sowohl technische als auch „soft skills“ abdecken. Dazu gehören Workshops, Online-Kurse und Weiterbildungsprogramme. [Bitte ergänzen Sie hier, wo Mitarbeiter Ihr Schulungsangebot einsehen und sich anmelden können]
3. **Dokumentation:** Nach Abschluss einer Schulung wird als eventueller Auditnachweis eine Teilnahmebestätigung gespeichert.
4. **Anwendung des Gelernten:** Wir ermutigen Sie, das in den Schulungen erlernte Wissen aktiv in Ihren Arbeitsalltag zu integrieren. Teilen Sie Ihre Erkenntnisse und Erfahrungen mit Ihrem Team, um den Wissenstransfer innerhalb der Abteilung zu fördern.
5. **Feedback:** Ihr Feedback ist uns wichtig. Geben Sie uns bitte nach Ihrer Schulung eine Bewertung und Kommentare zu Ihren Erlebnissen und dem Gelernten. Dies hilft uns, die Qualität und Relevanz unserer Schulungsangebote kontinuierlich zu verbessern.
6. **Unterstützung durch das Unternehmen:** Das Unternehmen stellt die notwendigen Ressourcen und Zeit zur Verfügung, damit Sie an den Schulungen teilnehmen können. Bei Fragen oder Problemen wenden Sie sich bitte an die Personalabteilung oder Ihren Vorgesetzten.

12.2 Disziplinarische Maßnahmen

Disziplinarische Maßnahmen sind ein wesentlicher Bestandteil einer fairen und transparenten Arbeitsumgebung. Sie dienen dazu, Fehlverhalten zu korrigieren, die Einhaltung von Unternehmensrichtlinien sicherzustellen und ein positives Arbeitsumfeld zu fördern. Diese Richtlinie legt die Grundsätze und Verfahren für disziplinarische Maßnahmen in unserem Unternehmen fest:

12.2.1 Grundsätze

- **Fairness und Transparenz:** Alle disziplinarischen Maßnahmen werden fair, konsistent und transparent durchgeführt.
- **Verhältnismäßigkeit:** Maßnahmen werden dem Fehlverhalten angemessen und verhältnismäßig sein.
- **Rechtliches Vorgehen:** Alle Maßnahmen erfolgen im Einklang mit geltenden Gesetzen und Tarifverträgen[sofern anwendbar].
- **Dokumentation:** Alle Schritte und Entscheidungen werden sorgfältig dokumentiert.

12.2.2 Stufen disziplinarischer Maßnahmen

Stufe 1 - Mündliche Ermahnung: Bei geringfügigen Verstößen erfolgt zunächst ein vertrauliches Gespräch zwischen dem Mitarbeiter und dem Vorgesetzten, um das Fehlverhalten zu besprechen und Lösungsmöglichkeiten zu finden.

Stufe 2 - Formelle Maßnahmen:

Schriftliche Verwarnung: Bei wiederholtem oder schwerwiegendem Fehlverhalten wird eine schriftliche Verwarnung ausgesprochen. Diese enthält eine Beschreibung des Fehlverhaltens, die erforderlichen Korrekturmaßnahmen und die Konsequenzen bei weiteren Verstößen.

Abmahnung: Eine oder mehrere schriftliche Abmahnungen erfolgen bei fortgesetztem Fehlverhalten. Eine Abmahnung dokumentiert das Fehlverhalten, gibt konkrete Anweisungen zur Verhaltensänderung und weist auf mögliche weitere disziplinarische Schritte hin.

Letzte Abmahnung: Vor einer möglichen Kündigung wird eine letzte Abmahnung ausgesprochen, die dem Mitarbeiter eine letzte Chance zur Verhaltensänderung gibt.

- **Stufe 3 - Disziplinarische Anhörungen:**
    - **Vorladung zur Anhörung:** Vor der Umsetzung schwerwiegender Maßnahmen, wie einer letzten Abmahnung oder Kündigung, wird der Mitarbeiter zu einer formellen Anhörung geladen. Der Mitarbeiter hat das Recht, eine Vertrauensperson hinzuzuziehen.
    - **Durchführung der Anhörung:** In der Anhörung werden die Vorwürfe erläutert und der Mitarbeiter erhält die Möglichkeit, seine Sichtweise darzulegen. Die Anhörung wird protokolliert.
- **Stufe 4 -Kündigung:**
    - **Ordentliche Kündigung:** Bei fortgesetztem Fehlverhalten trotz vorheriger Maßnahmen kann eine ordentliche Kündigung ausgesprochen werden. Die Kündigungsfrist wird eingehalten.
    - **Außerordentliche Kündigung:** Bei schwerwiegenden Verstößen, die eine weitere Zusammenarbeit unzumutbar machen, kann eine außerordentliche Kündigung ohne Einhaltung der Kündigungsfrist erfolgen.
- **Sonderfälle:**
    - **Mobbing und Diskriminierung:** Bei Vorwürfen von Mobbing, Diskriminierung oder Belästigung wird eine sofortige Untersuchung eingeleitet. Betroffene Mitarbeiter werden bis zur Klärung des Sachverhalts geschützt.
    - **Verstöße gegen Sicherheitsvorschriften:** Bei Verstößen gegen Sicherheitsvorschriften, die die Gesundheit oder Sicherheit gefährden, erfolgen sofortige Maßnahmen, einschließlich möglicher Freistellung des Mitarbeiters.

Alle disziplinarischen Maßnahmen werden schriftlich dokumentiert und in der Personalakte des Mitarbeiters archiviert. Dies umfasst Protokolle von Gesprächen, Anhörungen und schriftlichen Verwarnungen oder Abmahnungen.

12.2.3 Revision und Verbesserung disziplinarischer Maßnahmen

Die Richtlinien zu disziplinarischen Maßnahmen werden regelmäßig überprüft und bei Bedarf angepasst, um sicherzustellen, dass sie den aktuellen rechtlichen Anforderungen und den Bedürfnissen des Unternehmens entsprechen.

Alle Vorgesetzten werden regelmäßig in den Verfahren und Richtlinien zu disziplinarischen Maßnahmen geschult.

Mitarbeitern wird Unterstützung angeboten, um Fehlverhalten zu korrigieren, z. B. durch Schulungen, Übungen, Coaching oder externe Beratungsstellen.

13. Norm-Referenzen

13.1 Normreferenzen zu ISO27001:2022

Kapitel in diesem Dokument	Normkapitel (ISO27001:2022)
1. Einleitung	A 5.10
2. Gebrauch von Informationswerten	A 5.10; A 8.1
3. Klassifizierung und Kennzeichnung von Informationen	A 5.12; A 5.13

4. Übertragung von Werten: Intern/Extern, Surfen im Internet, Cloud Computing, Soziale Netzwerke	A 5.14; A 5.23
5. Aufbewahrung, Rückgabe & Löschung von Informationswerten, Entsorgung von Geräten	A 5.11; A 7.10; A 7.14; A 8.10
6. Schutz von geistigem Eigentum	A 5.32
7. Umgang mit künstlicher Intelligenz	./.
8. Identitäts- und Kennwortnutzung: Nutzung, Zugangsrechte, Prozesse	A5.16; A 5.17; A 5.18
9. Arbeiten innerhalb und außerhalb der Geschäftsräume: Aufgeräumter Arbeitsplatz, Endpunktgeräte, Geräteaufstellung,	A 6.7; A 7.2; A 7.3; A 7.6; A 7.7; A 7.8; A 7.9
10. Verhalten bei Ereignissen und Vorfällen: Meldungen, Meldekanäle	A 5.24; A 6.8
11. Schutz von Hinweisgebern (Whistleblowing)	./.
12. Schulung und Disziplinarische Maßnahmen bei Nicht-Einhaltung von Richtlinien	A 6.4; A 6.6

13.2 Referenzen zu TISAX-ISA 6.0

Kapitel in diesem Dokument	**Normkapitel (ISA-TISAX 6.0)**
1. Einleitung	1.1.1; 1.2.1
2. Gebrauch von Informationswerten	1.3.2; 2.1.3
3. Klassifizierung und Kennzeichnung von Informationen	1.3.2; 5.3.3
4. Übertragung von Werten: Intern/Extern, Surfen im Internet, Cloud Computing, Soziale Netzwerke	1.3.3 5.1.2; 5.3.4
5. Aufbewahrung, Rückgabe & Löschung von Informationswerten, Entsorgung von Geräten	3.1.1; 3.1.3; 3.1.4; 5.3.3; 7.1.2
6. Schutz von geistigem Eigentum	1.3.1; 7.1.1
7. Umgang mit künstlicher Intelligenz	./.
8. Identitäts- und Kennwortnutzung: Nutzung, Zugangsrechte, Prozesse	4.1.1; 4.1.3; 4.2.1
9. Arbeiten innerhalb und außerhalb der Geschäftsräume: Aufgeräumter Arbeitsplatz, Endpunktgeräte, Geräteaufstellung,	2.1.4; 3.1.4; 3.1.1
10. Verhalten bei Ereignissen und Vorfällen: Meldungen, Meldekanäle	1.6.1; 1.6.2; 5.1.1
11. Schutz von Hinweisgebern (Whistleblowing)	./.
12. Schulung und Disziplinarische Maßnahmen bei Nicht-Einhaltung von Richtlinien	1.1.1; 2.1.2