# Projektarbeit IHK Cyber Security Advisor

**Aufgabenstellung**:

Erstelle als Projektarbeit eine eigene Informationssicherheitsrichtlinie für ein fiktives Unternehmen. Wähle eine geeignete Richtlinienvorlage aus und arbeite diese entsprechend für dein fiktives Unternehmen und dessen Situation aus, um eine individuelle Richtlinie zu erstellen. Dabei sollten die bereitgestellten Richtlinien-Vorlagen genutzt werden. Diese stellen sicher, dass die formellen Anforderungen an die ISO27001 erfüllt sind. Das Dokument muss vor der eigentlichen Richtlinie eine Beschreibung deines fiktiven Unternehmens enthalten. Dort solltest du beschreiben wie z.B. bei einer Richtlinie über Netzwerksicherheit die Infrastruktur aktuell aussieht.

**Format**:

- Seitenanzahl: 10 Seiten (Deckblatt und Inhaltsverzeichnis zählen nicht zu den 10 Seiten)
- Schriftgröße: maximal 12 pt
- Dokumentenränder: Links und Rechts jeweils nicht breiter als 3 cm
- Formatvorlagen sind vorgegeben und sollten verwendet werden.

Autor: Lucian Haralambie
Datum: 09.01.2025
Kurs: WB CS_05

# Das Unternehmen

Die mittelständische Übersetzungsfirma **Translingua GmbH** mit Sitz in Frankfurt am Main beschäftigt rund 120 Mitarbeiter:innen. Das Unternehmen ist auf die Übersetzung sensibler Dokumente in den Bereichen Recht, Finanzen, Medizin und Technik spezialisiert. Dabei fallen hochvertrauliche Inhalte an, darunter juristische Unterlagen, technische Spezifikationen und personenbezogene Patientendaten. Ein Sicherheitsvorfall offenbarte erhebliche Schwachstellen beim Umgang mit Speichermedien.

# Szenario

**Problem 1: Unsachgemäßer Umgang mit internen Speichermedien**

- Dazu gehören: HDDs, SSDs oder Flash-Speicher in Servern, Laptops, mobilen Geräten oder Druckern
- Defekte oder auszutauschende Festplatten werden nicht über zertifizierte Drittanbieter entsorgt. Ein Vorfall zeigte, dass eine unsachgemäß entsorgte NAS-Festplatte von Cyberkriminellen ausgelesen und die Daten im Dark Web veröffentlicht wurden.
- Noch funktionsfähige Festplatten werden intern wiederverwendet, jedoch ohne vorherige sichere Datenlöschung. Dies birgt ein erhebliches Risiko, da sensible Informationen dabei wiederhergestellt werden könnten.

**Problem 2: Unkontrollierter Umgang mit externen Speichermedien**

- Dazu gehören: USB-Sticks, SD-Karten, USB-Festplatten, CDs/DVDs
- Aktuell dürfen Mitarbeiter:innen ohne Einschränkungen sowohl USB-Sticks und externe Festplatten als auch CDs/DVDs an ihren Windows-11-Laptops verwenden, und diese werden teils ohne geregeltes Verfahren entsorgt.

**Problem 3: Unzureichende Aktenvernichtung in Papierform**

- Es wurde festgestellt, dass nicht alle Papierdokumente einer Aktenvernichtung zugeführt werden, obwohl sie sensible Informationen enthalten können.
- Es fehlt ein standardisiertes Verfahren, das in jeder Abteilung die Aktenvernichtung sämtlicher zu entsorgender Unterlagen vorschreibt.

Diese Schwachstellen im Umgang mit Speichermedien und Dokumenten gefährden Datenschutz, Informationssicherheit und Compliance erheblich. Fehlende Maßnahmen bei Entsorgung und Aktenvernichtung erhöhen das Risiko einer unkontrollierten Offenlegung vertraulicher Informationen.

# IT-Infrastruktur

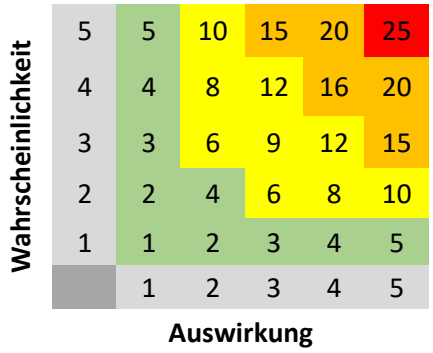
Die Translingua GmbH setzt auf eine hybride Implementierung, die Cloud-Dienste und On-Premise-Lösungen kombiniert, um Effizienz und Sicherheit zu gewährleisten.

**Cloud-Dienste:**
Microsoft Office 365 wird für die Kollaboration und Dokumentbearbeitung genutzt. DeepL unterstützt Übersetzungen, wobei sensible Daten nur in isolierten und gesicherten Umgebungen verarbeitet werden.

**On-Premise-Lösungen:**
Die Langzeit-Datenarchivierung erfolgt auf Synology NAS-Servern, die eine Wiederherstellbarkeit von bis zu 20 Jahren sicherstellen. Alle archivierten Daten werden durch Verschlüsselung geschützt und regelmäßige verschlüsselte Backups garantieren Datenintegrität.

**Endgeräte:**
Die Mitarbeiter:innen verwenden Windows 11 Laptops, die zentral von einem Windows Server verwaltet werden, der mittels Gruppenrichtlinien (GPOs) die Regeln durchsetzt.

# Risikoregister




| Level | Beschreibung | Wahrscheinlichkeit | Auswirkung |
|---|---|---|---|
| 1 | Sehr niedrig | < 1% | < 10k EUR |
| 2 | Niedrig | 1 - 5% | < 50k EUR |
| 3 | Mittel | 5 - 20% | < 250k EUR |
| 4 | Hoch | 20 - 50% | < 1M EUR |
| 5 | Kritisch | > 50% | > 1M EUR |

| Risiko-ID | Risiko | Auswirkung | Bewertung | Maßnahmen | Verantwortlich |
|---|---|---|---|---|---|
| R-1 | Unsachgemäße Entsorgung von Speichermedien | Wiederherstellung sensibler Daten durch Unbefugte | 4 (Hoch) | Einführung zertifizierter Verfahren zur physischen Zerstörung von Speichermedien | IT-Abteilung |
| R-2 | Unzureichende Datenlöschung bei Wiederverwendung von Festplatten | Wiederherstellung sensibler Daten aus wiederverwendeten Speichermedien | 3 (Mittel) | Einführung eines Prozesses, der bei Wiederverwendung sicherstellt, dass alle vorherigen Daten sicher gelöscht werden | IT-Abteilung |
| R-3 | Unkontrollierter Umgang mit externen Speichermedien | Datenverlust oder Offenlegung | 3 (Mittel) | Implementierung von GPO-Richtlinien zur Deaktivierung externer Schnittstellen und Einführung verschlüsselter Medien | IT-Abteilung |
| R-4 | Unzureichende Aktenvernichtung in Papierform | Offenlegung sensibler Informationen | 3 (Mittel) | Installation von Aktenvernichtungsgeräten (IT-Abteilung) und Einführung eines standardisierten Aktenvernichtungsverfahrens (HR-Abteilung) | IT-Abteilung, HR-Abteilung |
| R-5 | Mangelnde Schulung im Umgang mit Speichermedien | Fehlerhafte Handhabung | 2 (Niedrig) | Regelmäßige Schulungen und Sensibilisierungskampagnen zur sicheren Nutzung, Verschlüsselung und Entsorgung von Speichermedien | HR-Abteilung, IT-Abteilung |

Mit den beschriebenen Risiken und Maßnahmen abgeschlossen, folgt im nächsten Abschnitt die formelle Richtlinie zur sicheren Handhabung von Speichermedien.

**Translingua GmbH**

# RICHTLINIE FÜR SPEICHERMEDIEN

| | |
|---|---|
| Autor | Waylon Smithers |
| Letzter Bearbeiter | Lucian Haralambie |
| Erstellt am | 01.12.2024 |
| Bearbeitet am | 17.01.2025 |
| Dokumentenebene | Operativ |
| Zweck | Sicherstellung des ordnungsgemäßen Umgangs mit Speichermedien, um Datenverlust, Datenschutzverletzungen und Reputationsrisiken zu vermeiden |
| Sicherheitsklassifizierung | SK-1 (Intern) |
| Management-Kategorie | Informationssicherheit |
| Verantwortlicher | Waylon Smithers, CISO (Chief Information Security Officer) |
| Aktiv beteiligte Rollen | IT-Abteilung, HR-Abteilung, Facility-Abteilung, Datenschutzbeauftragter, Geschäftsführung |
| Passiv beteiligte Rollen | Mitarbeitende in den Bereichen Übersetzung, Verwaltung und Projektmanagement |
| Normkapitel ISO 9001 | 7.5 Dokumentierte Information |
| Normkapitel ISO 27001 | A.5.14, A.7.10, A.8.10, 6.3, 7.2.2 |
| Zuletzt intern auditiert | 09.01.2025 |

# Änderungs-Historie

| Datum | Version | Erstellt durch | Beschreibung der Änderung |
|---|---|---|---|
| 01.12.2024 | 0.1 | Waylon Smithers | Erster Entwurf des Dokuments |
| 02.12.2024 | 0.2 | Waylon Smithers | Formatanpassungen |
| 09.12.2024 | 1.0 | Max Mustermann | Aktualisierung der Verschlüsselungsvorgaben |
| 11.12.2024 | 1.1 | Lucian Haralambie | Einfügen neuer Prozesse zur Datenträgerlöschung |
| 16.12.2024 | 1.2 | Lucian Haralambie | Abschluss und finale Überprüfung der Richtlinie |
| 05.01.2025 | 1.3 | Lucian Haralambie | Weitere Korrekturen |
| 06.01.2025 | 1.4 | Lucian Haralambie | Feinabstimmung |
| 09.01.2025 | 1.5 | Lucian Haralambie | Finale Bearbeitung |
| 17.01.2025 | 1.6 | Lucian Haralambie | Detailing |
| | | | |

# Inhaltsverzeichnis

# 1. Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Dokuments ist die Erhöhung des Informationssicherheitsniveaus der Translingua GmbH durch klare Regeln für den sicheren Umgang mit sensiblen Informationen, Speichermedien (z. B. Festplatten, USB-Sticks, CDs/DVDs) und Papierdokumenten. Ziel ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Unternehmens- und Kundendaten sicherzustellen, indem Anforderungen und Maßnahmen für die Handhabung (Offenlegung, Veränderung, Entfernung, Archivierung und Zerstörung) definiert werden.

Diese Richtlinie gilt im Anwendungsbereich des ISMS der Translingua GmbH, Frankfurt am Main, und richtet sich an alle angestellten Mitarbeitenden sowie an externe Dritte, die Einrichtungen oder Informationen der Translingua GmbH nutzen. Sie umfasst den gesamten Lebenszyklus dieser Daten und Datenträger, von der Erstellung und Nutzung bis zur sicheren Archivierung und endgültigen Vernichtung. Anwender dieses Dokuments sind alle Mitarbeitenden der Translingua GmbH sowie relevante externe Parteien.

# 2. Referenzdokumente

- **ISO/IEC 27001:2022** Norm, Abschnitte:
  - A.5.14: Schutz bei der Übertragung von Informationen.
  - A.7.10: Umgang mit Wechselspeichermedien.
  - A.8.10: Ordnungsgemäße Löschung oder Zerstörung von Speichermedien.
  - 6.3: Informationssicherheitsbewusstsein und Schulung.
  - 7.2.2: Bewusstsein der Mitarbeiter:innen.

- **ISO/IEC 27002:2022**, **ISO/IEC 27701:2019** und **ISO/IEC 27005:2022** dienen als Leitfäden zur Umsetzung von ISO 27001-Kontrollen, Datenschutzmanagement (DSGVO-Compliance) und Risikomanagement in der Informationssicherheit.

- **DIN 66399**: Deutsche Norm für sichere Datenträgervernichtung (z. B. Papier, Festplatten, CDs/DVDs).

- **ISO/IEC 21964**: Internationaler Standard für die sichere physische Vernichtung von Datenträgern.

- **NIST 800-88**: Richtlinien des National Institute of Standards and Technology für sichere Datenlöschung.

- **FIPS 140-2**: Sicherheitsstandard für kryptografische Module.

- **ISO/IEC 19790**: Sicherheitsanforderungen für kryptografische Module.

- **BSI IT-Grundschutz Katalog**: Module:
  - ORP.3.3 Informationssicherheitsbewusstsein: Sensibilisierung und Schulung von Mitarbeiter:innen.
  - INF.4 Speichermedien: Umgang mit externen und internen Speichermedien.
  - OPS.1.2 Datensicherung: Regelungen zur sicheren Archivierung und Wiederherstellung.

- **Datenschutz-Grundverordnung (DSGVO)**:
  - Art. 5: Grundsätze der Verarbeitung (Vertraulichkeit und Integrität).
  - Art. 32: Sicherheit der Verarbeitung, z. B. Verschlüsselung und sichere Löschung.

- **ISO 31000**: Rahmenwerk für Risikomanagement.

- **ISO 22301**: Sicherstellung der Kontinuität kritischer Prozesse, z. B. Archivierung und Entsorgung.

# 3. Wechselspeichermedien

Die folgenden verbindlichen Maßnahmen regeln den sicheren Umgang mit Wechselspeichermedien, um das Risiko eines Informationsverlustes oder einer unbefugten Offenlegung zu minimieren:

Klassifizierung der Wechselspeichermedien:

- **Interne Medien**: Speichermedien, die fest in IT-Systemen verbaut oder direkt Teil der Geräte sind, wie Festplatten (HDD, SSD) in Servern, Laptops, Tablets, Multifunktionsgeräten oder Druckern.

- **Externe Medien**: Speichermedien, die physisch angeschlossen, entfernt oder transportiert werden können, wie USB-Sticks, externe Festplatten, SD-Karten, CDs, DVDs, Blu-rays oder ähnliche tragbare Medien.

- **Physische Medien**: Nicht-digitale Medien, die Informationen in physischer Form enthalten, wie Papierdokumente, Ausdrucke oder analoge Datenträger.

Diese Richtlinie ist von allen Mitarbeitenden und relevanten externen Parteien, die mit Wechselspeichermedien arbeiten, verbindlich einzuhalten. Sie stellt sicher, dass die Verwaltung, Nutzung, Aufbewahrung und Entsorgung der Medien den organisatorischen und rechtlichen Anforderungen entsprechen.

**Aufbewahrung und Schutz**
Alle Speichermedien müssen entsprechend ihrer Informationsklassifizierung (z. B. Intern, Vertraulich, Streng Vertraulich) in einer sicheren Umgebung aufbewahrt werden. Dabei sind Bedrohungen wie Hitze, Feuchtigkeit, Alterung oder elektronische Felder zu berücksichtigen. Die Lagerung erfolgt in Übereinstimmung mit den Herstellerspezifikationen, und physische Medien wie Papier sind in abschließbaren Schränken oder Tresoren zu sichern.

**Regelmäßige Überprüfungen**
Alle Wechselspeichermedien sind vierteljährlich (alle drei Monate) einer Überprüfung zu unterziehen. Die Verantwortung für die Durchführung dieser Überprüfungen liegt bei der IT-Abteilung, unterstützt durch den Datenschutzbeauftragten.

Die Überprüfung umfasst:
- Den Zustand der Speichermedien (z. B. auf Beschädigungen oder Alterung)
- Die Aktualität der gespeicherten Daten, um sicherzustellen, dass keine unlesbaren oder veralteten Medien verwendet werden
- Die Nachverfolgbarkeit aller registrierten Speichermedien gemäß den Dokumentationsanforderungen

Ergebnisse und Auffälligkeiten der Überprüfungen sind in einem Protokoll festzuhalten, welches die Maßnahmen zur Behebung von Problemen sowie die beteiligten Verantwortlichen dokumentiert. Das Protokoll ist vom Datenschutzbeauftragten zu prüfen und freizugeben.

**Registrierung und Nachverfolgbarkeit**
Alle Wechselspeichermedien sind zu registrieren, um deren Verbleib und Nutzung jederzeit nachverfolgen zu können. Die Registrierung umfasst mindestens:
- Typ des Speichermediums
- Nutzer oder verantwortliche Abteilung
- Verwendungszweck
- Aufbewahrungs- oder Nutzungszeitraum

**Zugriffskontrolle und Verschlüsselung**
Die Übertragung von Informationen auf Wechselspeichermedien ist zu überwachen und ausschließlich autorisierten Personen gestattet. Dabei muss sichergestellt werden, dass:

- Daten auf den Medien verschlüsselt sind
- keine unbefugten Zugriffe erfolgen können
- Passwörter oder Entschlüsselungsschlüssel sicher verwahrt werden

**Sicherer Transport**
Wenn Speichermedien oder physische Dokumente transportiert werden, sei es durch Mitarbeitende oder externe Dienstleister (z. B. Postdienste oder Kuriere), sind geeignete Sicherheitsmaßnahmen anzuwenden, darunter:

- Manipulationssichere Verpackung
- Verschlüsselung digitaler Daten
- Rückverfolgung des Transports durch Protokollierung und Empfangsbestätigungen

**Entsorgung und Wiederverwendung**
Nicht mehr benötigte Wechselspeichermedien sind gemäß den Richtlinien für sichere Wiederverwendung oder Entsorgung zu behandeln. Dies umfasst:

- Physische Zerstörung (z. B. Schreddern, Pulverisieren) oder sicheres Löschen von digitalen Speichermedien.
- Dokumentation aller Entsorgungs- oder Wiederverwendungsmaßnahmen gemäß den Anforderungen der ISO/IEC 27001.

**Besondere Maßnahmen für Papierdokumente**
Physische Medien wie Papierdokumente fallen ebenfalls unter die Richtlinie. Der sichere Umgang umfasst:

- Verschlossene Aufbewahrung, wenn nicht in Gebrauch
- Sicheres Schreddern oder Verbrennen bei Entsorgung
- Schutz bei Transport gemäß A.5.14 (Schutz bei der Übertragung von Informationen)

Diese verbindlichen Maßnahmen gewährleisten, dass alle Arten von Wechselspeichermedien sicher verwaltet, genutzt, transportiert und entsorgt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Informationen zu wahren.

## 3.1 Sichere Wiederverwendung oder Entsorgung

Für die sichere Wiederverwendung oder Entsorgung von Speichermedien sind folgende verbindliche Maßnahmen umzusetzen, um die Offenlegung sensibler Informationen gegenüber unbefugten Personen zu verhindern:

**Wiederverwendung von Speichermedien**
Speichermedien mit sensiblen Informationen, die innerhalb der Organisation wiederverwendet werden sollen, müssen vor der Wiederverwendung mit zertifizierter Software sicher gelöscht werden. Die sichere Löschung kann beispielsweise mit Methoden nach NIST 800-88 oder vergleichbaren Standards erfolgen. Alternativ ist eine vollständige Formatierung möglich, sofern sie den Sicherheitsanforderungen entspricht.
Dokumentation: Jeder durchgeführte Löschvorgang muss dokumentiert werden, um eine lückenlose Nachvollziehbarkeit gemäß ISO/IEC 27001 (A.8.10) sicherzustellen.

**Sichere Entsorgung von Speichermedien**
Speichermedien, die nicht mehr benötigt werden, müssen unverzüglich sicher entsorgt werden. Dies kann auf folgende Weise erfolgen:

- **Physische Zerstörung**: Schreddern, Pulverisieren oder mechanisches Bohren gemäß den Anforderungen der DIN 66399, die für die sichere physische Vernichtung von Datenträgern in Deutschland gilt. Diese Norm definiert Schutzklassen und Sicherheitsstufen, um eine Wiederherstellung der Daten zu verhindern. Zusätzlich ist die ISO/IEC 21964 ein internationaler Standard, der die physische Vernichtung von Datenträgern regelt und eng mit der DIN 66399 verbunden ist.
- **Sicheres Löschen**: Daten werden mit zertifizierten Methoden und Software unwiederbringlich gelöscht. Neben der DIN 66399, die sowohl physische Zerstörungsverfahren als auch digitale Löschmethoden berücksichtigt, ist der internationale Standard NIST 800-88 eine anerkannte

Richtlinie, die detaillierte Anforderungen für die Datenlöschung definiert. Diese wird weltweit als Referenz genutzt, insbesondere für die digitale Datenvernichtung.

**Externe Dienstleister**
Die Entsorgung und Zerstörung von Speichermedien muss ausnahmslos durch externe Dienstleister durchgeführt werden. Diese Dienstleister müssen nach ISO 9001 oder ISO/IEC 27001 zertifiziert sein. Der Dienstleister hat eine Entsorgungsbescheinigung vorzulegen, die den sicheren und datenschutzkonformen Umgang eindeutig dokumentiert.

**Identifikation und regelmäßige Überprüfung**
Ein Verfahren zur Identifikation von Speichermedien, die entsorgt oder wiederverwendet werden müssen, ist zu implementieren. Die Überprüfungen erfolgen vierteljährlich (alle drei Monate) und werden durch die IT-Abteilung in Zusammenarbeit mit dem Datenschutzbeauftragten durchgeführt. Während dieser Überprüfungen werden alle vorhandenen Datenträger inventarisiert und klassifiziert, um sicherzustellen, dass keine Speichermedien mit sensiblen Daten unbeabsichtigt zurückbleiben oder falsch entsorgt werden.

Ein Protokoll der Überprüfung ist anzufertigen und durch den Datenschutzbeauftragten zu unterzeichnen. Dabei sind festgestellte Auffälligkeiten, Maßnahmen zur Behebung sowie die Verantwortlichen klar zu dokumentieren.

**Protokollierung der Entsorgung**
Jede Entsorgung von Speichermedien mit sensiblen Informationen ist zu dokumentieren. Das Entsorgungsprotokoll muss folgende Informationen enthalten:

- Art des Datenträgers
- Methode der Entsorgung (z. B. Schreddern, Löschung, Pulverisierung)
- Zeitpunkt der Entsorgung
- Verantwortliche Person oder beauftragter Dienstleister

Die Protokolle dienen als Nachweis und ermöglichen einen vollständigen Prüfpfad im Rahmen von internen und externen Audits.

**Risikobeurteilung für beschädigte Medien**
Beschädigte Speichermedien, die sensible Daten enthalten, werden einer Risikobeurteilung durch die IT-Abteilung unterzogen. Auf Grundlage dieser Beurteilung wird entschieden, ob die Medien:

- physisch zerstört
- sicher zur Reparatur versandt oder
- endgültig ausgesondert werden

**Sicherstellung der Sicherheit**
Vor der Weitergabe an externe Dienstleister ist sicherzustellen, dass sensible Informationen nicht kompromittiert werden können.

Diese Maßnahmen garantieren, dass sensible Daten nicht in die Hände unbefugter Personen gelangen und alle gesetzlichen sowie organisatorischen Anforderungen eingehalten werden.

# 4. Kontrolle interner Datenträger

## 4.1 Verschlüsselung interner Speichermedien

Alle internen Datenträger (z. B. HDDs, SSDs, Flash-Speicher) müssen auf zwei Ebenen verschlüsselt werden, um maximale Sicherheit zu gewährleisten:

**Laptops**: Die Verschlüsselung erfolgt über Microsoft Windows Server-Gruppenrichtlinien (GPOs) in Kombination mit BitLocker. Diese Konfiguration stellt sicher, dass alle Betriebssystemlaufwerke verschlüsselt sind und zusätzliche Sicherheitsmaßnahmen, wie die Authentifizierung beim Start, aktiviert werden. Die IT-Abteilung implementiert und überwacht diese Richtlinien zentral und führt vierteljährlich Überprüfungen

durch, um die Einhaltung sicherzustellen. Abweichungen werden dokumentiert und behoben.

**NAS-Systeme**: Für Speichersysteme wie Synology NAS wird die Volumenverschlüsselung direkt in der DSM-Benutzeroberfläche aktiviert. Dabei wird sichergestellt, dass die Entschlüsselung ausschließlich mit einem sicheren, zentral gespeicherten Passwort oder Zertifikat erfolgt. Diese Konfiguration basiert auf den offiziellen Empfehlungen und Dokumentationen des Herstellers. Die IT-Abteilung überprüft diese Verschlüsselung vierteljährlich.

### 4.2 Kontrolle des Verschlüsselungsstatus

Der Verschlüsselungsstatus aller internen Datenträger wird monatlich durch die IT-Abteilung validiert, um sicherzustellen, dass keine unverschlüsselten Medien im Einsatz sind. Dabei wird auch die Integrität der Datenträger geprüft. Festgestellte Abweichungen werden dokumentiert und sofortige Maßnahmen zur Behebung eingeleitet.

## 5. Kontrolle externer Datenträger

### 5.1 Blockierung von Schnittstellen

Der Zugriff auf externe Datenträger wie USB-Sticks und SD-Karten wird durch zentrale Richtlinien blockiert, um unautorisierten Datenfluss zu verhindern. In der Windows-basierten Umgebung der Translingua GmbH erfolgt dies durch die Verwendung von Windows Server-Gruppenrichtlinien (GPOs), die zentral verwaltet und auf alle Endgeräte angewendet werden. Die IT-Abteilung stellt sicher, dass diese Konfiguration vierteljährlich überprüft und an aktuelle Sicherheitsanforderungen angepasst wird.

### 5.2 Zwangsverschlüsselung externer Datenträger

Externe Datenträger, die autorisiert genutzt werden, müssen vor ihrem Einsatz automatisch verschlüsselt werden. Dies wird über BitLocker To Go oder vergleichbare Technologien umgesetzt, die mit Windows Server-Gruppenrichtlinien konfiguriert werden. Die IT-Abteilung führt monatliche Prüfungen durch, um die Einhaltung dieser Anforderung sicherzustellen. Abweichungen werden dokumentiert und entsprechende Gegenmaßnahmen eingeleitet.

### 5.3 Ausnahmegenehmigungen

Die Nutzung externer Datenträger ist nur mit einer schriftlichen Ausnahmegenehmigung erlaubt. Diese muss den Verwendungszweck, die Dauer und die zugelassenen Geräte klar definieren. Die IT-Abteilung prüft vierteljährlich alle genehmigten Ausnahmen auf ihre Notwendigkeit und aktualisiert die zentrale Verwaltung entsprechend.

## 6. Kontrolle papierbasierter Medien

### 6.1 Sichere Aktenvernichtung

Alle papierbasierten Dokumente, die sensible Informationen enthalten, müssen gemäß den in diesem Dokument definierten Sicherheitsrichtlinien sicher vernichtet werden. Hierzu werden Aktenvernichter eingesetzt, die mindestens der Sicherheitsstufe P-4 nach DIN 66399 entsprechen. Diese Geräte zerkleinern Papier in so feine Partikel, dass eine Wiederherstellung der Informationen unmöglich ist. In Bereichen mit hohem Dokumentenaufkommen, wie den Rechts- oder Finanzabteilungen, werden zusätzliche Geräte bereitgestellt.

Aktenvernichter sind zentral und leicht zugänglich auf jeder Etage installiert. Für Bereiche ohne direkten Zugang zu einem Aktenvernichter stehen verschließbare Sammelbehälter zur Verfügung. Diese Behälter werden wöchentlich von autorisierten Mitarbeitern der Facility-Abteilung geleert, die gesammelten Dokumente werden sicher vernichtet und die ordnungsgemäße Durchführung wird protokolliert.

### 6.2 Standardisierte Prozesse zur Aktenvernichtung

Alle Mitarbeiter:innen sind verpflichtet, Papierdokumente mit vertraulichen Informationen nach Gebrauch unverzüglich in die vorgesehenen Aktenvernichter einzugeben. Der gesamte Prozess der Aktenvernichtung unterliegt vierteljährlichen stichprobenartigen Überprüfungen durch den Datenschutzbeauftragten. Dabei werden die Einhaltung der Richtlinien, die Funktionalität der Geräte sowie die Dokumentation geprüft.

Ergebnisse dieser Überprüfungen werden in einem Bericht festgehalten. Abweichungen werden in Zusammenarbeit mit den verantwortlichen Abteilungen analysiert und entsprechende Maßnahmen eingeleitet, um die Einhaltung der Sicherheitsstandards zu gewährleisten.

## 7. Überwachung und Auditierung

Die Einhaltung der Richtlinien wird durch regelmäßige Überwachung und interne sowie externe Audits sichergestellt. Gruppenrichtlinien werden zentral verwaltet und automatisch auf allen Endgeräten ausgerollt. Alle Zugriffe auf externe Datenträger sowie erteilte Genehmigungen werden protokolliert. Die IT-Abteilung überprüft diese Protokolle monatlich, um Verstöße oder Unregelmäßigkeiten frühzeitig zu erkennen und entsprechende Maßnahmen einzuleiten.

Halbjährlich werden umfassende interne Audits durch die IT-Abteilung durchgeführt, um sicherzustellen, dass die Sicherheitsrichtlinien korrekt implementiert und eingehalten werden. Diese Audits umfassen die Prüfung der Deaktivierung von Ports, die Nutzung externer Datenträger, den Verschlüsselungsstatus und die Einhaltung der Aktenvernichtungsprozesse. Externe Audits werden mindestens einmal jährlich durchgeführt, um die Einhaltung gesetzlicher Vorgaben und Best Practices zu validieren. Auffälligkeiten werden dokumentiert und mit den betroffenen Abteilungen besprochen, um Verbesserungspotenziale umzusetzen.

Schulungen und Sensibilisierungskampagnen fördern das Bewusstsein der Mitarbeiter:innen für sichere Arbeitsprozesse. Jährlich werden verpflichtende Schulungen durchgeführt, ergänzt durch Awareness-Maßnahmen wie Newsletter oder Aushänge. Neue Mitarbeiter:innen erhalten diese Schulung im Rahmen des Onboardings.

Verstöße gegen die Sicherheitsrichtlinien werden dokumentiert und mit der Personalabteilung besprochen, um angemessene disziplinarische Maßnahmen zu ergreifen. Diese Maßnahmen tragen dazu bei, die Einhaltung der Sicherheitsstandards zu gewährleisten und die Risiken für das Unternehmen zu minimieren.

# 8. Gültigkeit und Dokumenten-Handhabung

Dieses Dokument ist ab dem 09.01.2025 gültig. Der Eigentümer, der CISO, ist verpflichtet, das Dokument alle sechs Monate zu überprüfen und bei Bedarf zu aktualisieren. Bei der Bewertung der Wirksamkeit und Angemessenheit des Dokuments sind folgende Kriterien zu berücksichtigen:

a. Anzahl der Vorfälle im Zusammenhang mit der unsachgemäßen Handhabung von internen, externen und physischen Speichermedien.

b. Überprüfung der Einhaltung standardisierter Prozesse für die Datenlöschung, Entsorgung und sichere Aktenvernichtung.

c. Ergebnisse interner und externer Audits.

d. Einhaltung gesetzlicher Vorgaben.

Die Richtlinie wird allen Mitarbeitenden über das firmeneigene Intranet bereitgestellt. Neue Mitarbeitende erhalten eine Einführung im Rahmen des Onboardings.

CISO
Waylon Smithers