| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Fügen Sie hier den Namen der eingetragenen juristischen Person ein | | | | | | | |
| Dokumentnummer:<br>P12 | | | | | Dokumenttitel:<br>**Richtlinie zum Asset-Management** | | | | | | | |
| Version:<br>1.0 | | Datum des Inkrafttretens:<br>01.01.2025 | | | Dokumentenverantwortlicher: | | | | | | | |
| X | Richtlinie | | Standard | | Verfahren | | Formular | | Register | | Sonstiges | |

| **Änderungshistorie** | | | | |
|---|---|---|---|---|
| **Änderungsnummer** | **Änderungsdatum** | **Änderungen** | **Geprüft von** | **Prozessverantwortlicher** |
| | | | | |
| | | | | |

| **Genehmigungen** | | | |
|---|---|---|---|
| **Name** | **Position** | **Datum** | **Unterschrift** |
| | | | |
| | | | |

## 1. Zweck

1.1 Diese Richtlinie legt verbindliche organisatorische Anforderungen für die Identifizierung, Klassifizierung, Verwaltung und den Schutz von Informationswerten über deren gesamten Lebenszyklus fest. Sie unterstützt die unternehmensweite Governance von Hardware-, Software-, Daten-, Cloud- und immateriellen Informationswerten, einschließlich mobiler, ausgelagerter und durch Dritte verwalteter Umgebungen sowie Remote-Arbeitsumgebungen.

1.2 Zweck dieser Richtlinie ist es, vollständige Transparenz über die Informationswerte der Organisation sicherzustellen, um wirksame Sicherheitskontrollen, die Zuordnung von Verantwortlichkeiten, die Erfüllung von Compliance-Verpflichtungen sowie eine ordnungsgemäße Außerbetriebnahme oder Entsorgung zu gewährleisten.

1.3 Die Richtlinie ist an ISO/IEC 27001:2022 Anhang A, Maßnahme 5.9 ausgerichtet, indem sie die Führung eines zentralen Inventars von Informationen und zugehörigen Werten verbindlich vorschreibt. Sie stellt Rechenschaftspflicht sicher, indem jeder Wert einem Verantwortlichen zugeordnet und ein auf Klassifizierung, geschäftlicher Sensibilität sowie regulatorischen Anforderungen basierendes Schutzniveau angewendet wird.

## 2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Mitarbeitenden und Auftragnehmer sowie für externe Lieferanten und Dienstleister, die Informationswerte verwalten, nutzen, darauf zugreifen, diese speichern oder verarbeiten, sofern diese im Eigentum der Organisation stehen oder von ihr kontrolliert werden.

**2.2 Der Geltungsbereich umfasst alle Kategorien von Werten, darunter:**

2.2.1 Physische Werte: Laptops, Desktop-Systeme, mobile Endgeräte, Wechselmedien, Drucker, Netzwerkkomponenten

2.2.2 Digitale Werte: Software, Anwendungen, Systemabbilder, Datenbanken, Sicherungsdaten, Verschlüsselungsschlüssel

2.2.3 Informationswerte: strukturierte und unstrukturierte Daten, Berichte, E-Mails, geistiges Eigentum

2.2.4 Cloud- und virtuelle Werte: IaaS-, SaaS- und PaaS-Umgebungen, virtuelle Maschinen, Container

2.2.5 Logische Werte: Domänennamen, Lizenzen, Benutzerkonten, Baseline-Konfigurationen

2.3 Die Richtlinie regelt außerdem Werte, die im Rahmen von Remote-Arbeit, hybriden Arbeitsmodellen oder in ausgelagerten Umgebungen genutzt werden, und stellt Schutz und Transparenz auch dann sicher, wenn sich diese nicht physisch in den Räumlichkeiten der Organisation befinden.

## 3. Ziele

3.1 Aufrechterhaltung eines vollständigen, korrekten und aktuellen Inventars aller Informationswerte der Organisation mit festgelegten Angaben zu Verantwortlichkeit, Klassifizierung und Standort.

3.2 Benennung von Wertverantwortlichen, die für die Klassifizierung, Handhabung und den Schutz der Werte unter ihrer Verantwortung im Einklang mit dem Data-Governance-Modell und den Sicherheitsrichtlinien zuständig sind.

3.3 Anwendung einer angemessenen Klassifizierung und Kennzeichnung auf alle Werte auf Grundlage von Sensibilität, Kritikalität und regulatorischen Anforderungen.

3.4 Schutz von Werten entsprechend ihrer Klassifizierung und der damit verbundenen Risikoexposition, einschließlich Speicherung, Zugriff, Übertragung und Entsorgung.

3.5 Durchsetzung von Verfahren zur Rückgabe von Werten und zu deren sicherer Entsorgung im Rahmen des Offboardings, bei Vertragsbeendigung oder am Ende des Lebenszyklus eines Werts.

3.6 Unterstützung der Einhaltung regulatorischer und normativer Rahmenwerke wie ISO/IEC 27001, DSGVO, NIS2, DORA und COBIT 2019 durch strukturiertes Asset-Management und Auditierbarkeit.

**4. Rollen und Verantwortlichkeiten**

**4.1 Geschäftsleitung**

4.1.1 Genehmigt die Richtlinie zum Asset-Management und stellt sicher, dass die für ihre vollständige Umsetzung erforderlichen Ressourcen bereitgestellt werden.

4.1.2 Trägt die Gesamtverantwortung dafür, dass organisatorische Werte im Einklang mit regulatorischen und vertraglichen Verpflichtungen geschützt und verwaltet werden.

**4.2 Chief Information Security Officer (CISO)**

4.2.1 Ist für die Richtlinie zum Asset-Management verantwortlich und stellt deren Integration in das übergeordnete Informationssicherheits-Managementsystem (ISMS) der Organisation sicher.

4.2.2 Prüft Ausnahmen und Abweichungen von dieser Richtlinie und veranlasst risikobasierte Minderungsmaßnahmen.

4.2.3 Überwacht regelmäßige Audits der Asset-Klassifizierung, der Integrität des Asset-Inventars und der Einhaltung des Lebenszyklus von Informationswerten.

[ ... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ... ]

**9. Anforderungen an Überprüfung und Aktualisierung**

**9.1 Diese Richtlinie ist mindestens jährlich oder anlassbezogen zu überprüfen, insbesondere bei:**

9.1.1 Änderungen gesetzlicher oder regulatorischer Verpflichtungen, die Anforderungen an Asset-Klassifizierung oder Inventarisierung betreffen,

9.1.2 Einführung neuer Kategorien von Werten oder neuer Management-Plattformen (z. B. cloud-native CMDBs),

9.1.3 Feststellungen aus internen Audits oder Informationssicherheitsvorfällen im Zusammenhang mit mangelhafter Asset-Verwaltung,

9.1.4 organisatorischen Umstrukturierungen, die Verantwortlichkeiten oder Lebenszykluskontrollen betreffen.

9.2 Der Überprüfungsprozess ist vom IT Asset Manager einzuleiten und mit dem CISO, der Beschaffung, der Rechtsabteilung und den betroffenen Abteilungsleitern abzustimmen.

**9.3 Zwischenzeitliche Überprüfungen können außerdem ausgelöst werden durch:**

9.3.1 Erwerb oder Veräußerung von Geschäftseinheiten,

9.3.2 Änderungen bei Lieferanten, die von Dritten verwaltete Werte betreffen,

9.3.3 Technologieerneuerungen mit umfangreicher Außerbetriebnahme oder Bereitstellung.

**9.4 Alle Änderungen an dieser Richtlinie müssen:**

9.4.1 versionskontrolliert sein und im ISMS-Repository gespeichert werden,

9.4.2 von der Geschäftsleitung genehmigt werden,

9.4.3 eine Zusammenfassung der Änderungen und deren Begründung enthalten,

9.4.4 allen betroffenen Interessengruppen kommuniziert werden, einschließlich aktualisierter Verfahren oder Systemschulungen, soweit anwendbar.

**10. Verknüpfte Richtlinien und Bezüge**

**10.1 Diese Richtlinie gilt in Verbindung mit den folgenden zugehörigen Richtlinien und unterstützt deren Durchsetzung:**

10.1.1 P4 - Richtlinie zur Zugriffskontrolle: Stellt sicher, dass die Transparenz über Werte mit Zugriffsberechtigungen und Kontrollmechanismen über Systeme und Datenumgebungen hinweg abgestimmt ist.

10.1.2 P7 - Richtlinie für Onboarding und Austritt: Regelt die fristgerechte Bereitstellung und Rückgabe physischer und logischer Werte bei Personalwechseln.

10.1.3 P13 - Richtlinie zur Datenklassifizierung und Kennzeichnung: Legt verbindliche Klassifizierungsregeln für Werte fest, die Kennzeichnung, Handhabung und Entsorgungsverfahren bestimmen.

10.1.4 P14 - Richtlinie zur Datenaufbewahrung und Entsorgung: Definiert Zeitrahmen und Methoden für die sichere Entsorgung digitaler und physischer informationstragender Werte.

10.1.5 P22 - Richtlinie zur Protokollierung und Überwachung: Ermöglicht die Nachvollziehbarkeit von Zugriff und Nutzung von Werten durch Systemprotokollierung, Endpunkttransparenz und Verhaltensanalysen.

10.1.6 P30 - Incident-Response-Richtlinie (P30): Unterstützt die schnelle Eindämmung und Untersuchung von asset-bezogenen Verstößen, wie verlorenen Laptops oder nicht nachverfolgten Speichermedien.

10.2 Diese Richtlinien bilden eine zusammenhängende Governance-Struktur, die sicherstellt, dass Werte über ihren gesamten Lebenszyklus hinweg sicher verwaltet, korrekt inventarisiert und angemessen gehandhabt werden.

## 11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie ist an international anerkannten Informationssicherheitsstandards und regulatorischen Rahmenwerken ausgerichtet, die ein belastbares Asset-Management über den gesamten Lebenszyklus hinweg verlangen.

### 11.2 ISO/IEC 27001:

11.2.1 Abschnitt 8.1 - Verlangt von Organisationen, die Prozesse zu planen, umzusetzen und zu steuern, die erforderlich sind, um Anforderungen an die Informationssicherheit zu erfüllen, einschließlich solcher für das Lebenszyklusmanagement von Informationswerten.

### 11.3 ISO/IEC 27002:2022 - Maßnahmen 5.9 bis 5.11

11.3.1 Maßnahme 5.9 - Inventarisierung von Informationen und anderen zugehörigen Werten: Verlangt ein aktuelles und vollständiges Inventar aller für die Informationsverarbeitung relevanten Werte.

11.3.2 Maßnahme 5.10 - Zulässige Nutzung von Informationen und Werten: Wird durch Nutzungsregeln, Verantwortlichkeiten und Rückgabeprozesse unterstützt.

11.3.3 Maßnahme 5.11 - Rückgabe von Werten: Wird durch formale Übergabe- und Außerbetriebnahmeverfahren umgesetzt.

11.3.4 Diese Maßnahmen legen strukturierte Anforderungen für die Identifizierung, Kennzeichnung, Pflege und Nachverfolgung organisatorischer Werte sowie entsprechende Verantwortlichkeiten von Eigentümern und Verwahrern über den gesamten Lebenszyklus hinweg fest.

### 11.4 NIST SP 800-53 Rev.5:

11.4.1 CM-8 - System Component Inventory: Spiegelt sich in zentralem Asset-Management, Echtzeittransparenz und der Verknüpfung mit operativen Konfigurationen wider.

11.4.2 RA-3 - Risk Assessment: Asset-Inventare dienen als grundlegende Elemente für Bedrohungsmodellierung und Risikobewertung.

11.4.3 MP-6 - Media Sanitization: Wird durch sichere Entsorgungsmethoden durchgesetzt, die in den Kontrollen zum Asset-Lebenszyklus und in der Richtlinie zur Datenentsorgung festgelegt sind.

**11.5 EU-DSGVO (2016/679):**

11.5.1 Artikel 30 - Verzeichnis von Verarbeitungstätigkeiten: Verlangt von Organisationen, Systeme, Geräte und Speicherorte zu dokumentieren, die personenbezogene Daten speichern oder verarbeiten.

11.5.2 Artikel 32 - Sicherheit der Verarbeitung: Entspricht einer Asset-basierten Risikobewertung und Schutzmaßnahmen, die auf klassifizierte Werte und kritische Infrastrukturen zugeschnitten sind.

**11.6 EU-NIS2-Richtlinie (2022/2555):**

11.6.1 Artikel 21(2)(a, b): Schreibt Transparenz über Werte und Inventarisierung als Grundlage für Risikoanalyse, Schutz und Reaktion auf Cybersicherheitsvorfälle vor.

11.6.2 Artikel 21(3): Bekräftigt die Notwendigkeit einer strukturierten Asset-Governance als Teil einer organisatorischen Sicherheitskultur.

**11.7 EU-DORA (2022/2554):**

11.7.1 Artikel 5 - IKT-Governance und interne Kontrolle: Verlangt von Finanzunternehmen die Steuerung von IKT-Werten mit klaren Anforderungen an Inventarisierung, Verantwortlichkeit und Schutz.

11.7.2 Artikel 9 - IKT-Risikomanagementrahmen: Legt fest, dass Asset-Managementprozesse die Minderung von Bedrohungen, die Aufrechterhaltung des Geschäftsbetriebs und die Resilienz von Services unterstützen müssen.

**11.8 COBIT 2019:**

11.8.1 BAI09 - Manage Assets: Ist direkt auf die strukturierte Identifizierung, Klassifizierung, Nutzung und Entsorgung von Unternehmenswerten ausgerichtet.

11.8.2 DSS01 - Managed Operations: Unterstützt die Umsetzung von Kontrollen, die den Schutz von Werten und eine kontinuierliche operative Governance sicherstellen.

11.8.3 MEA03 - Monitor, Evaluate, and Assess Compliance: Stellt die regelmäßige Auditierung von Asset-Management-Kontrollen und ihrer Wirksamkeit in Bezug auf regulatorische Ausrichtung sicher.