					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P12S					Dokumenttitel: **Richtlinie zum Asset-Management**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

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

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

An Standards und Vorschriften ausgerichtet

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 8	Anforderungen an das Asset-Management
ISO/IEC 27002:2022	Maßnahme 5	Kontrollen für das Asset-Management
NIST SP 800-53 Rev.5	CM-8	Inventarisierung von Systemkomponenten
EU NIS2	Artikel 21(2)(a)	Asset-Nachverfolgung zum Schutz von Netz- und Informationssystemen
EU DORA	Artikel 5(8)	Anforderungen an das Inventar von IKT-Assets
COBIT 2019	BAI	Lebenszyklusmanagement von IT-Assets
DSGVO	Artikel 30	Verzeichnis von Verarbeitungstätigkeiten

1. Zweck

1.1 Diese Richtlinie legt fest, wie die Organisation ihre Informationswerte einschließlich physischer und digitaler Komponenten identifiziert, nachverfolgt, schützt und außer Betrieb nimmt.

1.2 Ziel ist es, betriebliche Risiken und Informationssicherheitsrisiken zu reduzieren, indem Transparenz, Verantwortlichkeit und ein sicherer Umgang mit allen geschäftlichen Assets über ihren gesamten Lebenszyklus sichergestellt werden.

1.3 Ein verlässliches Asset-Inventar unterstützt die Einhaltung regulatorischer Anforderungen, die Reaktion auf Sicherheitsvorfälle, die Kontinuitätsplanung und das Risikomanagement.

1.4 Diese Richtlinie unterstützt zudem die Zertifizierung nach ISO/IEC 27001 und weist die Ausrichtung an rechtlichen, finanziellen und cybersicherheitsbezogenen Verpflichtungen nach, unter anderem gemäß DSGVO, NIS2 und DORA.

1.5 Für kleine und mittlere Unternehmen (KMU) ist ein einfacher, aber systematischer Ansatz für das Asset-Management wesentlich, um nicht verwaltete Geräte, Datenverluste oder das Nichtbestehen von Audits zu vermeiden, insbesondere bei begrenzten personellen IT-Ressourcen.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Assets, die der Organisation gehören, von ihr geleast werden oder anderweitig von ihr verwaltet werden, einschließlich solcher, die verwendet werden für:

2.1.1 Büroarbeit

2.1.2 Remote-Arbeit oder hybride Arbeitsmodelle

2.1.3 Außendienst- oder mobile Tätigkeiten

2.1.4 Cloud- und ausgelagerte Umgebungen

2.2 Zu den erfassten Asset-Arten gehören unter anderem:

2.2.1 Hardware: Laptops, Desktop-Computer, Monitore, Telefone, Tablets, USB-Speichergeräte, Router, Drucker, Backup-Medien

2.2.2 Software: installierte Anwendungen, SaaS-Lösungen, Betriebssysteme, Antivirensoftware, Lizenzen

2.2.3 Daten-Assets: geschäftliche Datenspeicher, Tabellenkalkulationen, Kundendatensätze, Quellcode

2.2.4 Digitale Zugangsdaten und Dienste: Domainnamen, digitale Zertifikate, API-Schlüssel, E-Mail-Konten, Cloud-Anmeldeinformationen

2.2.5 Zugangsmedien: Schlüssel, Smartcards, Zutritts-Transponder, biometrische Token

2.3 Diese Richtlinie gilt für sämtliche Beschäftigten und Auftragnehmer sowie für Drittanbieter, die mit Assets der Organisation umgehen.

2.4 Die Richtlinie regelt sowohl kurzfristig genutzte Assets (z. B. projektspezifische Laptops) als auch langfristige Assets sowie gemeinsam genutzte Assets, die von mehreren Personen verwendet werden.

3. Ziele

3.1 Ein vollständiges und zutreffendes Inventar aller relevanten Assets ist einzurichten, aufrechtzuerhalten und fortlaufend zu aktualisieren.

3.2 Es ist sicherzustellen, dass jedem Asset ein benannter Verantwortlicher zugeordnet ist, der für Nutzung, Aufbewahrung und Rückgabe verantwortlich ist.

3.3 Assets sind auf Grundlage ihrer Sensitivität, ihrer geschäftlichen Auswirkung oder ihrer regulatorischen Relevanz zu klassifizieren, sodass abgestufte Schutzniveaus ermöglicht werden.

3.4 Es sind klare Verfahren für Ausgabe, Neuzuweisung, Wartung, Verlustmeldung und Außerbetriebnahme von Assets festzulegen.

3.5 Es ist sicherzustellen, dass Assets während ihres gesamten Lebenszyklus sicher gehandhabt werden und dass die darauf gespeicherten Informationen bei der Entsorgung entweder geschützt bleiben oder sicher gelöscht werden.

3.6 Die Wahrscheinlichkeit von Informationssicherheitsvorfällen infolge nicht nachverfolgter, nicht zurückgegebener oder missbräuchlich genutzter Ressourcen der Organisation ist zu reduzieren.

3.7 Die Einhaltung einschlägiger gesetzlicher Anforderungen, etwa des Rechenschaftsprinzips nach der DSGVO, sowie einschlägiger Standards für Cybersicherheitszertifizierungen ist zu unterstützen.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführung (GM)

4.1.1 Ist Eigentümer dieser Richtlinie und dafür verantwortlich, dass Asset-Management-Praktiken organisationsweit umgesetzt und eingehalten werden.

4.1.2 Prüft und genehmigt Aktualisierungen des Asset-Inventars und autorisiert erforderlichenfalls die Außerbetriebnahme oder Übertragung von Assets.

4.1.3 Ist über jeden wesentlichen Verlust, Diebstahl oder Missbrauch von Assets zu informieren.

4.2 IT-Leitung oder benannter Asset-Verantwortlicher

4.2.1 Pflegt das Asset-Inventar (z. B. in einer Tabellenkalkulation, einem Ticketsystem oder einem schlanken System zur Asset-Nachverfolgung).

4.2.2 Weist Verantwortlichkeiten für Assets zu und verfolgt Statusänderungen nach (z. B. neu, in Nutzung, in Reparatur, außer Betrieb genommen).

4.2.3 Überprüft, dass alle ausgegebenen Assets dokumentiert und einer Person oder einer Organisationseinheit zugeordnet sind.

4.2.4 Stellt sicher, dass Klassifizierungskennzeichnungen angewendet und eingehalten werden (z. B. Intern, Vertraulich).

4.2.5 Koordiniert Rückholung, Bereinigung und Deaktivierung von Assets im Rahmen des Offboardings oder der Außerbetriebnahme.

4.2.6 Meldet nicht aufgelöste Abweichungen im Asset-Bestand an die Geschäftsführung.

[... 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 einmal jährlich sowie immer dann zu überprüfen, wenn:

9.1.1 neue Arten von Technologien oder Assets eingeführt werden

9.1.2 sich Verfahren zur Asset-Nachverfolgung ändern (z. B. durch Einführung neuer Werkzeuge oder Plattformen)

9.1.3 neue regulatorische Verpflichtungen die Rückverfolgbarkeit oder Entsorgung von Assets betreffen

9.1.4 ein Sicherheitsvorfall oder Audit eine Lücke in den bestehenden Asset-Management-Praktiken identifiziert

9.2 An den Überprüfungen müssen die Geschäftsführung und die IT-Leitung beteiligt sein; sie müssen Aktualisierungen von Verfahren zum Umgang mit Assets, Inventarvorlagen und Leitlinien zur Klassifizierung umfassen.

9.3 Alle Aktualisierungen müssen dokumentiert und den betroffenen Beschäftigten mitgeteilt werden. Ein versionskontrolliertes Änderungsprotokoll ist aufzubewahren.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Weist Verantwortlichkeiten für Richtlinieneigentümerschaft und IT-Betrieb zu.

10.2 P4S – Richtlinie zur Zugriffskontrolle: Verknüpft die Nutzung von Assets (z. B. Laptops, mobile Geräte) mit Benutzerzugriffsrechten und dem Identitätsmanagement.

10.3 P7S – Richtlinie für Onboarding und Austritt: Stellt sicher, dass Ausgabe und Rückführung von Assets in Prozesse des Beschäftigungslebenszyklus integriert sind.

10.4 P13S – Richtlinie zur Datenklassifizierung und Kennzeichnung: Legt Regeln dafür fest, ob ein Asset als Intern oder Vertraulich zu klassifizieren ist.

10.5 P30S – Incident-Response-Richtlinie: Regelt Reaktionsverfahren, wenn ein assetbezogenes Ereignis zu einer Sicherheitsverletzung oder Datenschutzverletzung führt.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 8.1: Verlangt operative Kontrollen zur Verwaltung von Assets und zu deren Schutz während ihrer Nutzung.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 5.9: Beschreibt, wie Assets identifiziert, Verantwortlichkeiten zugewiesen, klassifiziert und sicher verwaltet werden.

11.3 NIST SP 800-53 Rev.5

11.3.1 CM-8: Verlangt von Organisationen, ein Inventar von Systemkomponenten einschließlich Hardware, Software und virtueller Assets zu erstellen und aufrechtzuerhalten.

11.4 DSGVO

11.4.1 Artikel 30: Verlangt die Dokumentation von Verarbeitungstätigkeiten, wofür bekannt sein muss, wo Daten gespeichert sind und auf welchen Assets sie sich befinden.

11.5 EU NIS2

11.5.1 Artikel 21(2)(a): Fordert technische und organisatorische Maßnahmen, einschließlich der Asset-Nachverfolgung, zum Schutz von Netz- und Informationssystemen.

11.6 EU DORA

11.6.1 Artikel 5(8): Finanzunternehmen müssen als Teil des Managements von IKT-Risiken detaillierte Inventare von IKT-Assets führen.

11.7 COBIT 2019

11.7.1 BAI09: Legt fest, dass IT-Assets über ihren gesamten Lebenszyklus hinweg – von der Beschaffung bis zur Außerbetriebnahme – mit klaren Verantwortlichkeiten und Kontrollen verwaltet werden müssen.