					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P13S					Dokumenttitel: **Richtlinie zur Datenklassifizierung und Kennzeichnung**							
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**

Ausgerichtet an Standards und Vorschriften

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 5.3, 8	
ISO/IEC 27002:2022	Maßnahmen 5.12, 5.13	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
EU NIS2	Artikel 21(2)(a)	
EU DORA	Artikel 5(8)	
COBIT 2019	BAI03.05, DSS05	
DSGVO	Artikel 5, 32	

1. Zweck

1.1 Diese Richtlinie legt fest, wie sämtliche von der Organisation verarbeiteten Informationen zu klassifizieren und zu kennzeichnen sind, um ihre Vertraulichkeit, Integrität und Verfügbarkeit (CIA) über den gesamten Lebenszyklus sicherzustellen.

1.2 Sie gewährleistet eine einheitliche Datenverarbeitung, indem Informationen auf Grundlage ihrer Sensibilität, ihrer geschäftlichen Auswirkungen oder rechtlicher Verpflichtungen angemessenen Schutzstufen zugeordnet werden.

1.3 Klassifizierung und Kennzeichnung tragen dazu bei, das Risiko einer unbeabsichtigten Offenlegung, eines unbefugten Zugriffs oder eines unsachgemäßen Umgangs mit sensiblen Daten zu reduzieren, insbesondere in KMU, die sich gegebenenfalls auf einfachere Systeme und weniger formalisierte Kontrollen stützen.

1.4 Diese Richtlinie ist wesentlich für die Zertifizierung nach ISO/IEC 27001 und die Einhaltung regulatorischer Anforderungen, insbesondere im Hinblick auf Datenschutzgesetze wie die DSGVO sowie Cybersicherheitsrahmenwerke wie NIS2 und DORA.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für sämtliche Daten der Organisation, unabhängig von Format oder Speicherort, einschließlich:

2.1.1 elektronischer Dokumente, Tabellen, E-Mails, Formulare, Bilder und gescannter Dateien

2.1.2 physischer Dokumente wie Ausdrucke, Berichte, Rechnungen und Notizen

2.1.3 Daten, die in Cloud-Diensten, auf lokalen Servern, Wechselmedien oder auf für geschäftliche Zwecke genutzten persönlichen Geräten gespeichert oder verarbeitet werden

2.1.4 temporärer oder flüchtiger Daten, die im Rahmen des Geschäftsbetriebs erzeugt werden, z. B. Protokolle, Cache-Dateien und E-Mails

2.2 Sämtliche Mitarbeitenden, Auftragnehmenden, Zeitarbeitskräfte und externen Dienstleister mit Zugriff auf Daten der Organisation müssen diese Richtlinie einhalten.

2.3 Sie gilt über den gesamten Datenlebenszyklus hinweg – von der Erstellung und Speicherung über Zugriff und Übermittlung bis hin zu Archivierung oder Löschung.

3. Ziele

3.1 Festlegung eines einfachen, durchsetzbaren Klassifizierungsschemas, das in der gesamten Organisation leicht verständlich und anwendbar ist.

3.2 Verpflichtung, jeden Datenbestand und jeden Informationswert entsprechend seiner Sensibilität zu klassifizieren und angemessen zu kennzeichnen, um einen sachgerechten Umgang, eine angemessene Speicherung und einen angemessenen Zugriff zu steuern.

3.3 Sicherstellung, dass Kennzeichnungspraktiken in Geschäftsabläufe wie Onboarding, Projektinitiierung und Systemeinrichtung integriert sind.

3.4 Reduzierung des Risikos von Datenschutzverletzungen durch Anwendung von Kontrollen für den Umgang mit Daten, z. B. Verschlüsselung und Zugriffsbeschränkungen, entsprechend der Klassifizierungsstufe.

3.5 Sicherstellung der Einhaltung von Datenschutz- und Informationssicherheitsvorgaben durch den Nachweis, dass sensible Daten, z. B. personenbezogene, finanzielle oder proprietäre Informationen, ordnungsgemäß gekennzeichnet und verwaltet werden.

3.6 Etablierung klarer Rechenschaftspflichten für Klassifizierungsentscheidungen sowie Sicherstellung regelmäßiger Überprüfungen und Aktualisierungen auf Grundlage sich ändernder geschäftlicher und rechtlicher Anforderungen.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführung (GM)

4.1.1 ist Eigentümerin dieser Richtlinie und genehmigt das Klassifizierungsschema.

4.1.2 stellt die Aufsicht sicher, damit Verantwortlichkeiten für die Klassifizierung zugewiesen und durchgesetzt werden.

4.1.3 muss Ausnahmen von Klassifizierungs- oder Kennzeichnungsanforderungen prüfen und genehmigen.

4.1.4 stellt sicher, dass Praktiken zum Umgang mit Daten die Compliance-Anforderungen aus Gesetzen wie der DSGVO und DORA erfüllen.

4.2 Informationswerteigentümer / Datenmanager

4.2.1 weist jedem neuen Datenbestand oder Informationswert bei Erstellung oder Beschaffung eine initiale Klassifizierung zu.

4.2.2 stellt sicher, dass sichtbare Kennzeichnungen, z. B. Dateikopfzeilen, Fußzeilen, Wasserzeichen oder Ordnernamen, soweit anwendbar verwendet werden.

4.2.3 überprüft Klassifizierungen regelmäßig auf Relevanz, Genauigkeit und erforderliche Änderungen, z. B. nach Herabstufung oder Veröffentlichung.

4.2.4 arbeitet mit der IT-Leitung zusammen, um technische Schutzmaßnahmen auf Grundlage der Klassifizierung durchzusetzen, z. B. Zugriffsrechte und Verschlüsselung.

[... 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 muss jährlich durch den GM und den Datenmanager überprüft werden, um sicherzustellen, dass sie Folgendes berücksichtigt:

9.1.1 Änderungen im Geschäftsbetrieb oder bei Datenarten

9.1.2 neue regulatorische Anforderungen, z. B. zum Datenschutz oder zur Finanzaufsicht

9.1.3 technologische Veränderungen, die Kennzeichnungs- oder Klassifizierungsfähigkeiten beeinflussen

9.2 Die Überprüfung muss Aktualisierungen der Klassifizierungskategorien, Kennzeichnungswerkzeuge oder -praktiken sowie der Sensibilisierungs- und Schulungsinhalte umfassen.

9.3 Überarbeitungen dieser Richtlinie müssen durch den GM genehmigt und sämtlichem Personal mitgeteilt werden. Eine Versionshistorie muss für Audit-Zwecke aufbewahrt werden.

10. Verwandte Richtlinien und Verknüpfungen

10.1 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Weist Rechenschaftspflichten für Eigentümerschaft und Durchsetzung von Richtlinien zu.

10.2 P4S – Richtlinie zur Zugriffskontrolle: Richtet den Systemzugriff an den Datenklassifizierungsstufen aus.

10.3 P12S – Richtlinie zum Asset-Management: Erfasst die physischen und digitalen Werte, auf denen klassifizierte Daten gespeichert werden.

10.4 P17S – Richtlinie zu Datenschutz und Privatsphäre: Regelt den Schutz personenbezogener Daten, von denen ein erheblicher Teil als vertraulich klassifiziert ist.

10.5 P30S – Incident-Response-Richtlinie: Legt Eskalationswege und Reaktionsverfahren bei Klassifizierungsverstößen oder Datenoffenlegungen fest.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 5.3: verlangt klar definierte Verantwortlichkeiten für Datenverarbeitung und Schutz.

11.1.2 Klausel 8.1: fordert operative Planung und Kontrollen, einschließlich solcher im Zusammenhang mit der Datenklassifizierung.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 5.12: enthält Leitlinien zur Informationsklassifizierung auf Grundlage von Risiko- und Regulierungsanforderungen.

11.2.2 Maßnahme 5.13: beschreibt praktische Mechanismen zur Kennzeichnung und die zugehörigen Regeln für den Umgang.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: fordert die Kennzeichnung von Informationen, damit Schutzmaßnahmen der Klassifizierung entsprechen.

11.3.2 MP-3 / MP-5: enthalten Leitlinien zur Kennzeichnung und Kontrolle von Medien und Ausgaben.

11.4 DSGVO

11.4.1 Artikel 5 und 32: verlangen Datenminimierung und Integrität durch angemessene Klassifizierungs- und Schutzmaßnahmen im Umgang mit Daten.

11.5 EU NIS2

11.5.1 Artikel 21(2)(a): schreibt technische und organisatorische Kontrollen für einen risikobasierten Schutz vor.

11.6 EU DORA

11.6.1 Artikel 5(8): verpflichtet Unternehmen, Datenbestände als Teil ihres IKT-Risikomanagementprogramms zu klassifizieren.

11.7 COBIT 2019

11.7.1 BAI03.05: fordert Informationsklassifizierung und risikoadäquaten Schutz.

11.7.2 DSS05.02: behandelt die Durchsetzung klassifizierungsbasierter Kontrollen und deren Überwachung.