					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P13					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**

1. Zweck

1.1 Diese Richtlinie definiert den formalen Rahmen für die Klassifizierung und Kennzeichnung von Informationswerten der Organisation auf Grundlage von Sensibilität, Risikoexposition und regulatorischen Verpflichtungen.

1.2 Sie stellt sicher, dass sämtliche Informationen – unabhängig davon, ob sie gespeichert, übertragen oder verarbeitet werden – eindeutig kategorisiert und so gekennzeichnet werden, dass das erforderliche Schutzniveau und die entsprechenden Anforderungen an die Handhabung klar erkennbar sind.

1.3 Diese Richtlinie schreibt eine strukturierte Klassifizierung vor, die an den Risikomanagementpraktiken der Organisation ausgerichtet ist, und unterstützt die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit (CIA) über digitale und physische Datenarten hinweg.

1.4 Diese Maßnahme ist wesentlich, um rollenbasierten Zugriff, Auditfähigkeit, angemessene Datenweitergabe sowie die wirksame Umsetzung technischer Maßnahmen wie Verschlüsselung, Datensicherung und Überwachung zu ermöglichen.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle Informationswerte der Organisation, einschließlich Dokumenten, Datenbanken, Aufzeichnungen und Kommunikation,

2.1.2 alle Datenformate, einschließlich digitaler, gedruckter, schriftlicher oder mündlicher Form,

2.1.3 alle Umgebungen: lokal, remote, mobil und in der Cloud,

2.1.4 alle Mitarbeitenden, Auftragnehmer, Dienstleister und Auftragsverarbeiter Dritter, die Informationen der Organisation erstellen, verarbeiten oder speichern.

2.2 Der Geltungsbereich umfasst intern entwickelte Inhalte, extern bezogene Daten, personenbezogene Daten im Rahmen datenschutzrechtlicher Verpflichtungen (z. B. DSGVO) sowie Informationen, die mit Kunden, Partnern und Aufsichtsbehörden ausgetauscht werden.

2.3 Sie gilt für alle Systeme, die zur Speicherung oder Übertragung von Daten verwendet werden, einschließlich Unternehmensanwendungen, Dateiservern, E-Mail-Systemen, Cloud-Plattformen und Backup-Speichern.

3. Ziele

3.1 Etablierung eines standardisierten, organisationsweit einheitlichen Klassifizierungsschemas auf Grundlage der Auswirkungen einer Offenlegung oder Kompromittierung von Daten.

3.2 Sicherstellung, dass alle Informationen sichtbar und dauerhaft gekennzeichnet werden, um ihre Klassifizierungsstufe und die Anforderungen an ihre Handhabung abzubilden.

3.3 Durchsetzung von Kontrollen für Datenverarbeitung und Zugriff entsprechend der Klassifizierung, einschließlich Verschlüsselung, Protokollierung, Übertragungsschutz und Aufbewahrungsplanung.

3.4 Unterstützung der Einhaltung internationaler Standards (ISO/IEC 27001, 27002), regulatorischer Rahmenwerke (DSGVO, NIS2, DORA) und interner Risikorichtlinien.

3.5 Sicherstellung, dass alle Benutzer ihre Verantwortlichkeiten beim Schutz von Daten, bei der Anwendung von Kennzeichnungen und beim korrekten Umgang mit klassifizierten Informationen verstehen.

3.6 Aufrechterhaltung der Rückverfolgbarkeit zwischen Klassifizierungsstatus, zugehörigen Kontrollen und dem Asset-Inventar der Organisation für Audit- und Compliance-Zwecke.

4. Rollen und Verantwortlichkeiten

4.1 Chief Information Security Officer (CISO)

4.1.1 Ist verantwortlich für die Richtlinie zur Informationsklassifizierung und Kennzeichnung und stellt sicher, dass sie mit regulatorischen, vertraglichen und betrieblichen Anforderungen im Einklang steht.

4.1.2 Genehmigt Klassifizierungsstufen, Kennzeichnungsstandards und Änderungen an der Richtlinie.

4.1.3 Überwacht die Einhaltung der Richtlinie anhand von Audits, Kennzahlen und Ausnahmereviews.

4.1.4 Koordiniert die funktionsübergreifende Governance mit Rechtsabteilung, Datenschutz und Risikomanagement.

4.2 Informationswerteigentümer

4.2.1 Sind für die Klassifizierung der Informationswerte in ihrem Verantwortungsbereich anhand des Klassifizierungsschemas der Organisation verantwortlich.

4.2.2 Wenden Klassifizierungskennzeichnungen bei Erstellung, Aktualisierung oder Übernahme an.

4.2.3 Überprüfen die Klassifizierung von Informationswerten regelmäßig, insbesondere bei Änderungen der Sensibilität, des regulatorischen Geltungsbereichs oder des geschäftlichen Werts.

4.2.4 Stellen sicher, dass sensible Daten während ihres gesamten Lebenszyklus angemessen behandelt und gekennzeichnet werden.

[... 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 zu überprüfen, um die Ausrichtung an Folgendem sicherzustellen:

9.1.1 sich weiterentwickelnden regulatorischen Anforderungen (z. B. DSGVO, NIS2, DORA),

9.1.2 Aktualisierungen der Leitlinien zur Klassifizierung in ISO/IEC 27001 oder 27002,

9.1.3 organisatorischen Änderungen mit Auswirkungen auf Datensensibilität oder Eigentümerschaft,

9.1.4 technologischen Änderungen, einschließlich neuer Plattformen für Dokumenten- oder Datenmanagement.

9.2 Der Chief Information Security Officer (CISO) muss die Überprüfung in Zusammenarbeit mit dem Informationssicherheitsausschuss, der Rechtsabteilung und betroffenen Geschäftsbereichen veranlassen.

9.3 Überprüfungen müssen Folgendes umfassen:

9.3.1 die Wirksamkeit der Durchsetzung der Klassifizierung und die Einhaltung durch Benutzer,

9.3.2 die Analyse von Vorfällen oder Ausnahmen im Zusammenhang mit Fehlklassifizierungen,

9.3.3 Benutzerrückmeldungen zu Kennzeichnungswerkzeugen oder Leitlinienmaterialien,

9.3.4 Benchmarking anhand branchenüblicher Klassifizierungsstandards.

9.4 Aktualisierungen der Richtlinie müssen versionskontrolliert, im ISMS-Dokumentenregister dokumentiert und allen relevanten Mitarbeitenden mit besonderem Fokus auf neue Verantwortlichkeiten oder Änderungen an Werkzeugen mitgeteilt werden.

9.5 Neue Mitarbeitende müssen während des Onboardings mit der aktuellen Version dieser Richtlinie vertraut gemacht werden. Alle Mitarbeitenden müssen nach wesentlichen Richtlinienänderungen Auffrischungsschulungen absolvieren.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie wird unmittelbar unterstützt durch und setzt Kontrollen aus den folgenden zugehörigen Richtlinien durch:

10.1.1 P4 - Richtlinie zur Zugriffskontrolle: Der Zugriff auf Informationen wird durch Klassifizierungsstufen gesteuert; sensiblere Daten erfordern strengere Zugriffskontrollen und Autorisierungsmechanismen.

10.1.2 P11 - Richtlinie zur Verwaltung von Benutzerkonten und Berechtigungen: Verstärkt die Vergabe von Berechtigungen auf Basis des Need-to-know-Prinzips, das durch Klassifizierungsstufen bestimmt wird.

10.1.3 P12 - Richtlinie zum Asset-Management: Stellt sicher, dass jedes Asset im Inventar seine Klassifizierung und Kennzeichnung enthält und dadurch Rückverfolgbarkeit und Rechenschaftspflicht unterstützt werden.

10.1.4 P14 - Richtlinie zur Datenaufbewahrung und Entsorgung: Entsorgungs- und Aufbewahrungsregeln werden durch die Klassifizierungsstufe der Daten und regulatorische Aufbewahrungspflichten bestimmt.

10.1.5 P18 - Richtlinie zu kryptografischen Maßnahmen: Wendet geeignete Verschlüsselungsstandards entsprechend der Klassifizierung des Informationswerts an.

10.1.6 P22 - Richtlinie zur Protokollierung und Überwachung: Ermöglicht die Überwachung von Zugriffen auf und Bewegungen von klassifizierten Informationen und stellt Auditierbarkeit sowie die Erkennung von Fehlkennzeichnungen oder Missbrauch sicher.

10.2 Jede Verknüpfung gewährleistet einen konsistenten Schutz von Informationen über ihren gesamten Lebenszyklus hinweg, von der Erstellung und Klassifizierung bis zur sicheren Handhabung, Speicherung, Übertragung und endgültigen Vernichtung.

11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie ist an international anerkannten Standards und regulatorischen Rahmenwerken zur Klassifizierung und Kennzeichnung sensibler Informationen ausgerichtet.

11.2 ISO/IEC 27001

11.2.1 Abschnitt 4.2 - Verstehen der Erfordernisse und Erwartungen interessierter Parteien. Klassifizierungsanforderungen ergeben sich häufig aus rechtlichen, regulatorischen oder vertraglichen Verpflichtungen, die von interessierten Parteien auferlegt werden (z. B. DSGVO, Kunden-NDAs), und müssen in dieser Richtlinie berücksichtigt werden.

11.2.2 Abschnitt 6.1.3 - Informationssicherheitsrisikobehandlung. Die Klassifizierung beeinflusst unmittelbar die Auswahl von Kontrollen zur Risikobehandlung, einschließlich Zugriffskontrolle, Verschlüsselung und Aufbewahrung, auf Grundlage der Datensensibilität.

11.2.3 Abschnitt 7.2 - Kompetenz. Diese Richtlinie schreibt vor, dass Personal, das für Klassifizierung und Kennzeichnung verantwortlich ist, geschult sein muss; dies fällt unter die Kompetenzanforderungen.

11.2.4 Abschnitt 7.3 - Sensibilisierung. Diese Richtlinie verlangt, dass sich alle Benutzer der Klassifizierungsstufen und ihrer Verantwortlichkeiten beim Umgang mit Informationen bewusst sind, im Einklang mit den Sensibilisierungsanforderungen.

11.2.5 Abschnitt 7.5 - Dokumentierte Information. Die Klassifizierungsrichtlinie selbst ist ein gelenktes Dokument, und Verfahren, Schulungsnachweise sowie Klassifizierungskennzeichnungen sind Teil der dokumentierten Information.

11.2.6 Abschnitt 8.1 - Operative Planung und Steuerung. Klassifizierung und Kennzeichnung sind operative Prozesse, die in das Management des Datenlebenszyklus eingebettet sind; diese Anforderung stellt sicher, dass solche Tätigkeiten geplant, umgesetzt und gesteuert werden.

11.2.7 Abschnitt 9.1 - Überwachung, Messung, Analyse und Bewertung. Diese Richtlinie enthält Regelungen zur Überwachung der Einhaltung der Klassifizierung, zu Trends bei Sicherheitsvorfällen und zur Wirksamkeit des Kennzeichnungsschemas.

11.2.8 Abschnitt 10.1 - Nichtkonformität und Korrekturmaßnahme. Diese Richtlinie definiert Reaktionen auf Fehlklassifizierungen, einschließlich Korrekturmaßnahmen wie Nachschulungen, Aktualisierungen und Ausnahmenbehandlung.

11.3 ISO/IEC 27002:2022

11.3.1 Maßnahme 5.12 - Klassifizierung von Informationen. Diese Maßnahme stellt sicher, dass Informationen anhand ihrer Sensibilität, ihres Werts und ihrer Kritikalität klassifiziert werden – genau dies wird durch diese Richtlinie formalisiert.

11.3.2 Maßnahme 5.13 - Kennzeichnung von Informationen. Diese Maßnahme verlangt eine angemessene Kennzeichnung von Informationen entsprechend ihrer Klassifizierungsstufe; dies wird in dieser Richtlinie umfassend behandelt.

11.3.3 Maßnahme 5.10 - Zulässige Nutzung von Informationswerten und anderen zugehörigen Vermögenswerten. Diese Richtlinie legt fest, wie Benutzer mit klassifizierten Daten umzugehen haben, unterstützt damit die zulässige Nutzung und verhindert Missbrauch.

11.3.4 Maßnahme 5.11 - Rückgabe von Vermögenswerten. Die Klassifizierung trägt dazu bei, dass sensible Daten identifiziert und bei Austritt eines Mitarbeiters oder Lieferanten sicher zurückgegeben oder bereinigt werden.

11.3.5 Maßnahme 5.9 - Inventarisierung von Informationswerten und anderen zugehörigen Vermögenswerten. Die Klassifizierung ist häufig mit dem Asset-Inventar verknüpft, das die Klassifizierungsstufe jedes Eintrags abbilden muss, um eine angemessene Zuweisung von Kontrollen zu unterstützen.

11.3.6 Maßnahme 5.14 - Informationsübertragung. Klassifizierungsstufen beeinflussen die Kontrollen für interne und externe Datenübermittlungen (z. B. Verschlüsselung, Genehmigung, Zugriffsbeschränkungen).

11.3.7 Maßnahme 8.12 - Verhinderung von Datenabfluss. Die Durchsetzung von Klassifizierung und Kennzeichnung unterstützt die Verhinderung unbefugter Offenlegung und von Datenverlust.

11.3.8 Maßnahme 8.11 - Datenmaskierung. Bestimmte Klassifizierungsstufen (z. B. Vertraulich, Streng vertraulich) können eine Maskierung erfordern, wenn Daten in Test-/Entwicklungsumgebungen oder Analysen verwendet werden.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Richtlinie und Verfahren zum Schutz von Systemen und Kommunikation: Unterstützt Klassifizierungsrichtlinien als Teil des übergreifenden Datenschutzes.

11.4.2 AC-16 - Sicherheitsattribute: Setzt die Zugriffsdurchsetzung auf Grundlage von Klassifizierungsmetadaten und Benutzerberechtigungen um.

11.4.3 MP-3 / MP-5 - Kennzeichnung von Datenträgern und Schutz beim Transport: Erzwingt Kennzeichnung und Schutz von Daten bei Speicherung und Übertragung entsprechend ihrer Klassifizierung.

11.5 EU GDPR (2016/679)

11.5.1 Artikel 5 - Grundsätze für die Verarbeitung personenbezogener Daten: Verlangt, dass personenbezogene Daten sicher und ihrer Sensibilität angemessen verarbeitet werden.

11.5.2 Artikel 32 - Sicherheit der Verarbeitung: Bestärkt die Klassifizierung als Mechanismus für risikobasierten Datenschutz und angemessene technische Maßnahmen.

11.6 EU NIS2 Directive (2022/2555)

11.6.1 Artikel 21(2)(a): Verlangt Richtlinien für das Informationssicherheitsrisikomanagement, einschließlich Kontrollen zur Asset- und Datenklassifizierung.

11.6.2 Artikel 21(3): Fördert die Einführung von Maßnahmen zur Durchsetzung angemessener Datenverarbeitung, unterstützt durch klassifizierungsbasierte Kennzeichnung.

11.7 EU DORA (2022/2554)

11.7.1 Artikel 5 - Governance und Kontrolle: Verlangt Governance-Rahmenwerke, die Datenbestände für die Steuerung von IKT-Risiken klassifizieren.

11.7.2 Artikel 9 - IKT-Risikomanagement: Schreibt technische und organisatorische Maßnahmen für kritische IKT-Assets vor, einschließlich Klassifizierung und Kennzeichnung.

11.8 COBIT 2019

11.8.1 DSS05.02 - DSS05 Sicherheitsdienste verwalten: Erzwingt Informationssicherheitsklassifizierungen, um den Schutz von Unternehmensdaten sicherzustellen.

11.8.2 MEA03 - Überwachen, Evaluieren und Beurteilen der Einhaltung: Unterstützt regelmäßige Audits und Überprüfungen von Klassifizierungspraktiken, um Richtlinieneinhaltung und Reifegrad sicherzustellen.