					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P08S					Dokumenttitel: **Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit**							
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 relevanten Standards und Vorschriften ausgerichtet

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 7	
ISO/IEC 27002:2022	Maßnahme 6	
NIST SP 800-53 Rev. 5	AT-2, AT-4	
EU-NIS2	Artikel 21(2)(i)	
EU DORA	Artikel 13	
COBIT 2019	BAI08, DSS	
EU-DSGVO	Artikel 32, 39	

1. Zweck

1.1. Diese Richtlinie stellt sicher, dass sämtliche Mitarbeitenden und Auftragnehmer ihre Verantwortlichkeiten in Bezug auf die Informationssicherheit verstehen.

1.2. Sie dient dazu, die Wahrscheinlichkeit menschlicher Fehler zu verringern, die Fähigkeit zur Erkennung und Meldung von Sicherheitsvorfällen zu verbessern und eine sicherheitsbewusste Kultur in der gesamten Organisation zu fördern.

1.3. Die Richtlinie unterstützt die Einhaltung von ISO/IEC 27001, NIS2, DSGVO und DORA, indem sie das Sicherheitsbewusstsein als Bestandteil des täglichen Arbeitsverhaltens und der rollenspezifischen Erwartungen verankert.

2. Geltungsbereich

2.1. Diese Richtlinie gilt für sämtliche Mitarbeitenden, Auftragnehmer, Praktikanten und Dritte, die Zugriff auf Unternehmenssysteme oder Daten haben.

2.2. Sie umfasst:

2.2.1. die Einweisung neuer Beschäftigter in die Informationssicherheit,

2.2.2. die jährliche Auffrischungsschulung zur Informationssicherheit,

2.2.3. anlassbezogene Sensibilisierungsmaßnahmen (z. B. vorfallsbezogene Aktualisierungen, Poster oder Hinweise).

2.3. Sie gilt für alle Rollen, Abteilungen und Arbeitsorte.

3. Ziele

3.1. Sicherstellen, dass alle Mitarbeitenden rechtzeitig verständliche und relevante Schulungen zur Informationssicherheit erhalten.

3.2. Mitarbeitende in die Lage versetzen, häufige Bedrohungen wie Phishing, Schadsoftware und Datenabfluss zu erkennen und zu vermeiden.

3.3. Eine Dokumentation der Schulungsabschlüsse bereitstellen, um die Einhaltung rechtlicher, vertraglicher und prüfungsbezogener Anforderungen nachzuweisen.

3.4. Schulungsinhalte aktuell halten, damit sie den Richtlinien, Bedrohungen und anwendbaren Vorschriften der Organisation entsprechen.

3.5. Eine proaktive Haltung unter den Mitarbeitenden fördern, bei der Sicherheit als Teil der täglichen Verantwortung verstanden wird.

4. Rollen und Verantwortlichkeiten

4.1. Geschäftsführer (GM)

4.1.1. Genehmigt Schulungsanforderungen und stellt sicher, dass die erforderlichen Ressourcen bereitgestellt werden.

4.1.2. Prüft Berichte zu Schulungsabschlüssen und eskaliert Verstöße bei Bedarf.

4.2. Office Manager / Personalabteilung

4.2.1. Koordiniert die Durchführung von Schulungen für Neueinstellungen und jährlichen Auffrischungsschulungen.

4.2.2. Führt Schulungsnachweise und Abschlussprotokolle.

4.2.3. Stellt sicher, dass Mitarbeitende die Kenntnisnahme wesentlicher Informationssicherheitsrichtlinien und Geheimhaltungsvereinbarungen (NDA) bestätigen.

[... 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. Jährliche Überprüfung

9.1.1. Diese Richtlinie muss jährlich durch den Geschäftsführer (GM) und die Personalabteilung überprüft werden, um sicherzustellen, dass sie den aktuellen Risiken, regulatorischen Anforderungen und Anforderungen der Belegschaft entspricht.

9.2. Zwischenzeitliche Aktualisierungen

9.2.1. Richtlinie und Schulungsinhalte müssen außerdem überprüft und überarbeitet werden nach:

9.2.1.1. einem erheblichen Sicherheitsvorfall,

9.2.1.2. rechtlichen oder vertraglichen Änderungen,

9.2.1.3. organisatorischen Umstrukturierungen oder Systemmigrationen.

9.3. Versionskontrolle und Verteilung

9.3.1. Jede Aktualisierung muss Folgendes enthalten:

9.3.1.1. Versionsnummer und Datum des Inkrafttretens,

9.3.1.2. Zusammenfassung der Änderungen,

9.3.1.3. Genehmigung durch den Geschäftsführer (GM),

9.3.1.4. ein Archiv aller früheren Versionen, das mindestens drei Jahre aufbewahrt wird.

9.4. Kommunikation an Mitarbeitende

9.4.1. Aktualisierungen der Richtlinie müssen allen Mitarbeitenden mitgeteilt werden; bei wesentlichen Änderungen ist eine Bestätigung einzuholen.

10. Verwandte Richtlinien und Verknüpfungen

10.1. Diese Richtlinie unterstützt Folgendes:

10.1.1. P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Weist die Verantwortung für Schulungskoordination und Aufsicht zu.

10.1.2. P3S – Richtlinie zur zulässigen Nutzung: Verstärkt die in der Schulung vermittelten Verhaltenserwartungen.

10.1.3. P4S – Zugriffsrichtlinie: Stellt sicher, dass Benutzer die Bedeutung der Zugriffssicherheit verstehen.

10.1.4. P7S – Richtlinie für Onboarding und Austritt: Verankert Schulungen im Eintrittsprozess.

10.1.5. P30S – Richtlinie zur Reaktion auf Sicherheitsvorfälle (P30): Stellt sicher, dass Mitarbeitende wissen, wie Vorfälle zeitnah und korrekt gemeldet werden.

11. Referenzstandards und Rahmenwerke

11.1. ISO/IEC 27001

11.1.1. Klausel 7.3 – Verlangt, dass Organisationen sicherstellen, dass sich das Personal seiner Verantwortlichkeiten und der Auswirkungen auf die Sicherheit bewusst ist.

11.2. ISO/IEC 27002

11.2.1. Maßnahme 6.3 – Beschreibt die Erwartungen an Umfang und Durchführung von Sicherheitsschulungen.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AT-2 – Verlangt Sensibilisierungsschulungen für Benutzer mit Systemzugriff.

11.3.2. AT-4 – Behandelt rollenbasierte Schulungen und Folgen bei Nichteinhaltung.

11.4. EU-DSGVO

11.4.1. Artikel 32 – Verlangt Sicherheitsmaßnahmen einschließlich Mitarbeiterschulungen zum Schutz personenbezogener Daten.

11.4.2. Artikel 39 – Verlangt, dass Datenschutzbeauftragte (DPO) gegebenenfalls Sensibilisierung und Schulung überwachen.

11.5. EU-NIS2-Richtlinie

11.5.1. Artikel 21(2)(i) – Verlangt fortlaufende Sensibilisierungsprogramme und Schulungen zur Cybersicherheit.

11.6. EU DORA

11.6.1. Artikel 13 – Verlangt, dass Finanzunternehmen Schulung und Weiterbildung für sämtliches Personal mit IKT-bezogenen Verantwortlichkeiten umsetzen.

11.7. COBIT 2019

11.7.1. BAI08 – Wissen verwalten: Stellt sicher, dass Mitarbeitende kompetent und geschult sind.

11.7.2. DSS05 – Sicherheitsdienste verwalten: Hebt Sensibilisierung als wesentliche Schutzmaßnahme hervor.