					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P08					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 7.3, Anhang A Maßnahme 6.3	Legt Anforderungen an Sensibilisierung und Schulung fest, die durch diese Richtlinie adressiert werden
ISO/IEC 27002:2022	Maßnahme 6	Unterstützt angemessene, rollenbasierte Sensibilisierung und Schulung
NIST SP 800-53 Rev.5	AT-1 bis AT-5	Entspricht Anforderungen an Richtlinien und Verfahren, Sensibilisierungsschulungen, rollenspezifische Schulungen, Schulungsnachweise und den Kontakt zu Sicherheitsgruppen
DSGVO	Artikel 32, 39; Erwägungsgrund 78	Verlangt Schulungen für Personen, die personenbezogene Daten verarbeiten, sowie die allgemeine Sensibilisierung des Personals
NIS2-Richtlinie	Artikel 21(2)(a, b), 21(3)	Verlangt Richtlinien zu Risiko- und Sicherheitsschulungen sowie Sensibilisierungsinitiativen
DORA	Artikel 5, 8, 13	Verlangt IKT-Risikobewusstsein und Schulungen als Teil von Resilienzmaßnahmen
COBIT 2019	APO07 Personalmanagement, DSS05 Sicherheitsdienste verwalten, MEA03 Überwachen, Evaluieren und Beurteilen der Compliance	Verstärkt die Sensibilisierung der Belegschaft, Benutzerschulung und die Überwachung der Einhaltung

1. Zweck

1.1 Diese Richtlinie legt den formalen Rahmen fest, um sicherzustellen, dass sämtliches Personal über seine Verantwortlichkeiten im Bereich der Informationssicherheit informiert ist und die erforderlichen Schulungen erhält, um die Vertraulichkeit, Integrität und Verfügbarkeit (CIA) von Informationswerten zu schützen.

1.2 Sie unterstützt ISO/IEC 27001, Klausel 7.3, und Anhang A, Maßnahme 6.3, indem sie ein strukturiertes und risikobasiertes Sensibilisierungs- und Schulungsprogramm vorschreibt, das auf organisatorische Rollen und sich entwickelnde Bedrohungen zugeschnitten ist.

1.3 Die Richtlinie trägt dazu bei, menschlich bedingte Schwachstellen zu reduzieren, sicherheitsbewusstes Verhalten zu fördern und sichere Praktiken fortlaufend im Einklang mit regulatorischen und vertraglichen Anforderungen zu verankern.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle internen und externen Personen mit Zugriff auf Informationssysteme, Daten oder Einrichtungen der Organisation, einschließlich:

2.1.1 Mitarbeitende (Vollzeit, Teilzeit, befristet beschäftigt)

2.1.2 Auftragnehmer, Berater, Lieferanten und Praktikanten

2.1.3 Dritte mit logischem oder physischem Zugriff im Rahmen von Servicevereinbarungen

2.2 Der Geltungsbereich umfasst:

2.2.1 Erstschulung zur Sensibilisierung für Informationssicherheit

2.2.2 Rollenspezifische Schulungen (z. B. für Entwickler, Finanzpersonal, hochprivilegierte Benutzer)

2.2.3 Regelmäßige Auffrischungen und Sensibilisierungskampagnen

2.2.4 Ad-hoc-Schulungen als Reaktion auf Vorfälle oder neue Bedrohungen

2.3 Zu den von dieser Richtlinie abgedeckten Schulungsformaten gehören E-Learning, persönliche Briefings, Simulationen, Wissensprüfungen, Poster, Sicherheitsnewsletter und verpflichtende Bestätigungen.

3. Ziele

3.1 Sicherzustellen, dass sämtliches Personal seine Verantwortlichkeiten beim Schutz organisatorischer Werte und bei der Einhaltung von Sicherheitsrichtlinien versteht.

3.2 Fortlaufende, messbare Sensibilisierung und Schulung bereitzustellen, die an die rollenbasierte Risikoexposition angepasst sind.

3.3 Sichere Verhaltensweisen in den täglichen Betrieb zu integrieren, indem Praktiken wie sichere Passwortnutzung, Vorfallmeldung und Widerstandsfähigkeit gegenüber Phishing gestärkt werden.

3.4 Die regulatorische Einhaltung und Auditbereitschaft im Hinblick auf Pflichten zur Informationssicherheitsschulung über Branchen und Rechtsräume hinweg sicherzustellen.

3.5 Sicherheitsvorfälle, die aus Fahrlässigkeit, mangelnder Sensibilisierung oder Fehlentscheidungen resultieren, durch Verhaltenssteuerung und kontinuierliche Verstärkung zu reduzieren.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung

4.1.1 Genehmigt die Strategie der Organisation für Schulung und Sensibilisierung im Bereich Informationssicherheit und stellt sicher, dass hierfür ausreichende Ressourcen bereitgestellt werden und diese in den Unternehmensprioritäten verankert ist.

4.1.2 Überwacht die Einhaltung auf Managementebene und setzt die Befolgung dieser Richtlinie in allen Abteilungen durch.

4.2 CISO / ISMS-Manager

4.2.1 Verantwortet diese Richtlinie und definiert den Rahmen für Sensibilisierung und Schulung im Einklang mit Risiko-, Compliance- und Geschäftsanforderungen.

4.2.2 Überwacht Konzeption, Bereitstellung, Nachverfolgung und Überprüfung aller Maßnahmen zur Schulung in Informationssicherheit.

4.2.3 Stellt sicher, dass Schulungen regelmäßig aktualisiert werden und sich entwickelnde Bedrohungen sowie neue Technologien berücksichtigen.

[... 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 Überprüfungsfrequenz

9.1.1 Diese Richtlinie und das zugehörige Schulungsprogramm müssen überprüft werden:

9.1.1.1 jährlich oder

9.1.1.2 nach schwerwiegenden Vorfällen infolge menschlichen Fehlers oder einer Insider-Bedrohung

9.1.1.3 bei Einführung wesentlicher neuer Technologien oder Bedrohungen

9.1.1.4 als Reaktion auf Änderungen rechtlicher, vertraglicher oder zertifizierungsbezogener Verpflichtungen

9.2 Überprüfungsprozess

9.2.1 Die Überprüfung wird durch den CISO in Abstimmung mit folgenden Stellen geleitet:

9.2.1.1 Personal- und Schulungsabteilungen

9.2.1.2 Rechtsabteilung und Datenschutzbeauftragter

9.2.1.3 Funktionen für IT-Sicherheit und operationelles Risiko

9.2.2 Alle Aktualisierungen müssen:

9.2.2.1 durch den Informationssicherheitslenkungsausschuss genehmigt werden

9.2.2.2 versionskontrolliert und im ISMS-Dokumentenregister dokumentiert werden

9.2.2.3 den Benutzern mitgeteilt werden, wenn wesentliche Änderungen den Schulungsumfang oder Verantwortlichkeiten betreffen

9.3 Governance für Inhaltsaktualisierung

9.3.1 Schulungsmodule und Sensibilisierungsmaterialien müssen alle 12 Monate überprüft werden, um Folgendes sicherzustellen:

9.3.1.1 Relevanz für die Bedrohungslage

9.3.1.2 regulatorische Richtigkeit

9.3.1.3 Formatkompatibilität (z. B. Barrierefreiheit, Lokalisierung)

9.3.2 Veraltete oder irreführende Inhalte müssen unverzüglich zurückgezogen und durch genehmigte Alternativen ersetzt werden.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie wird unterstützt durch und unterstützt die Durchsetzung von:

10.1.1 P01 – Informationssicherheitsrichtlinie: Legt Sicherheitsbewusstsein als grundlegende Maßnahme im ISMS der Organisation fest.

10.1.2 P03 – Richtlinie zur zulässigen Nutzung: Verlangt im Rahmen von Schulungen eine Richtlinienbestätigung durch Benutzer und präzisiert Verantwortlichkeiten für die tägliche Nutzung von Technologien.

10.1.3 P07 – Richtlinie für Onboarding und Austritt: Stellt sicher, dass Schulungen beim Eintritt verankert und während des gesamten Beschäftigungslebenszyklus nachverfolgt werden.

10.1.4 P06 – Risikomanagement-Richtlinie: Verknüpft menschenzentrierte Schulungen mit Bedrohungsmodellierung und Strategien zur Reduzierung von Restrisiken.

10.1.5 P33 – Richtlinie zur Audit- und Compliance-Überwachung: Validiert, dass Sensibilisierungskontrollen im Rahmen von Audits operativ, messbar und wirksam sind.

10.2 Zusammen bilden diese Richtlinien ein umfassendes Rahmenwerk für verhaltensorientierte Kontrollen, das Sensibilisierung, Rechenschaftspflicht und kulturelle Verankerung integriert.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 7.3 – Sensibilisierung: Verlangt, dass Organisationen sicherstellen, dass Beschäftigte die Informationssicherheitsrichtlinien und ihre Verantwortlichkeiten kennen. Diese Richtlinie setzt diese Anforderung durch strukturiertes Onboarding, regelmäßige Schulungen und messbare Teilnahme an Kampagnen operativ um.

11.1.2 Anhang A Maßnahme 6.3 – Sensibilisierung, Ausbildung und Schulung zur Informationssicherheit: Wird vollständig durch initiale, rollenbasierte und fortlaufende Schulungsprogramme adressiert, die auf die Risikoprofile der Benutzer zugeschnitten sind.

11.2 ISO/IEC 27002:2022 – Maßnahme 6

11.2.1 Unterstützt die Entwicklung und Bereitstellung von Sensibilisierung und Schulung, die den jeweiligen Aufgaben entsprechen, mit Schwerpunkt auf der Verstärkung sicheren Verhaltens und regelmäßigen Aktualisierungen auf Grundlage von Bedrohungsinformationen und Audit-Rückmeldungen.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 bis AT-5 (Familie Awareness and Training): Diese Richtlinie entspricht AT-1 (Richtlinie und Verfahren), AT-2 (Sensibilisierungsschulung), AT-3 (rollenspezifische Schulung), AT-4 (Nachweise zu Sicherheitsschulungen) und AT-5 (Kontakt mit Sicherheitsgruppen).

11.3.2 IA-5, AC-2: Verstärkt die Verantwortung der Benutzer für sichere Authentifizierung und zulässige Nutzung – zentrale Elemente der Verhaltensergebnisse von Sensibilisierungsprogrammen.

11.3.3 IR-1 bis IR-8: Die Incident-Response-Bereitschaft wird durch gezielte Sensibilisierungskampagnen und Simulationen gestärkt.

11.4 DSGVO (2016/679)

11.4.1 Artikel 32 – Sicherheit der Verarbeitung: Verlangt, dass Personal, das personenbezogene Daten verarbeitet, darauf geschult wird, Risiken für personenbezogene Daten zu erkennen, zu verhindern und zu melden. Diese Richtlinie stellt sicher, dass Datenverarbeiter und alle relevanten Rollen entsprechend geschult werden.

11.4.2 Artikel 39 – Aufgaben des Datenschutzbeauftragten: Umfasst die Sensibilisierung und Schulung von Personal, das an Verarbeitungsvorgängen beteiligt ist.

11.4.3 Erwägungsgrund 78: Empfiehlt angemessene Sensibilisierungsmaßnahmen, um robuste Sicherheitspraktiken und die Befolgung von Richtlinien sicherzustellen.

11.5 NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(a, b): Verlangt von Einrichtungen, Richtlinien zur Risikoanalyse und Sicherheitsschulung für sämtliches relevantes Personal einzuführen. Diese Richtlinie erfüllt diese Anforderung durch die Einführung kontinuierlicher, rollensensitiver Schulungsprozesse.

11.5.2 Artikel 21(3): Fördert die Sensibilisierung für Cybersicherheitsrisiken bei Management und Personal durch Sensibilisierungsinitiativen und Simulationen.

11.6 DORA (2022/2554)

11.6.1 Artikel 13 – Strategie für digitale operationelle Resilienz: Verlangt, dass IKT-Risikobewusstsein und Schulungen Teil des Governance-Modells sind. Diese Richtlinie stellt sicher, dass menschliche Risiken durch fortlaufende Schulung und Bedrohungssimulation adressiert werden.

11.6.2 Artikel 5 und 8: Betonen die Bedeutung interner Kontrollrahmen, zu deren grundlegenden Bestandteilen Sensibilisierung und Schulung für IKT-Resilienz und Cyberhygiene gehören.

11.7 COBIT 2019

11.7.1 APO07 Personalmanagement – Managed Human Resources: Verstärkt die Notwendigkeit, das Bewusstsein für Sicherheitsverantwortlichkeiten zu entwickeln und dies in das Personalmanagement einzubetten.

11.7.2 DSS05 Sicherheitsdienste verwalten – Managed Security Services: Legt Kontrollen für Benutzerschulung und Vorfallmeldung fest, die beide integraler Bestandteil dieser Richtlinie sind.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: Verlangt die Überprüfung der Wirksamkeit von Benutzerverhalten und Richtlinieneinhaltung – hier umgesetzt durch Phishing-Tests, Quizze und Kennzahlen zu Sensibilisierungskampagnen.