					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P18S					Dokumenttitel: **Richtlinie zu kryptografischen Kontrollen**							
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**

Ausrichtung an Standards und Vorschriften

Standard/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 8	
ISO/IEC 27002:2022	Maßnahmen 8.24, 8.25	
NIST SP 800-53 Rev. 5	SC-12 bis SC-17	
EU NIS2	Artikel 21(2)(d), 21(2)(e)	
EU DORA	Artikel 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
EU DSGVO	Artikel 32(1)(a), 34	

1. Zweck

1.1 Diese Richtlinie legt verbindliche Anforderungen für den Einsatz von Verschlüsselung und kryptografischen Kontrollen zum Schutz der Vertraulichkeit, Integrität und Authentizität geschäftlicher und personenbezogener Daten fest.

1.2 Sie stellt sicher, dass kryptografische Werkzeuge in Systemen, auf Endgeräten und in Cloud-Diensten in einer Kleinunternehmensumgebung angemessen eingesetzt werden.

1.3 Diese Richtlinie unterstützt unmittelbar die Zertifizierung nach ISO/IEC 27001:2022 und hilft der Organisation, die gesetzlichen Verpflichtungen aus der EU-Datenschutz-Grundverordnung (DSGVO), der EU-NIS2-Richtlinie und dem Digital Operational Resilience Act (DORA) zu erfüllen.

1.4 Zu den abgedeckten kryptografischen Kontrollen zählen Datenverschlüsselung, Zertifikatsmanagement, die sichere Handhabung von Schlüsseln und verschlüsselte Backups.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle Mitarbeitenden, Auftragnehmer und Dritten, die Unternehmensdaten verarbeiten,

2.1.2 alle Geschäftsanwendungen, Endgeräte und Cloud-Plattformen, die zum Speichern, Übertragen oder Abrufen vertraulicher Informationen genutzt werden,

2.1.3 alle personenbezogenen, finanziellen, rechtlichen oder anderweitig sensiblen Aufzeichnungen, die gemäß der Richtlinie zur Datenklassifizierung und Kennzeichnung klassifiziert sind,

2.1.4 sämtliche kryptografischen Kontrollen, einschließlich Verschlüsselungsverfahren, Schlüsseln, Passwörtern, Zertifikaten und Sicherheitsmodulen.

2.2 Die Richtlinie umfasst ruhende Daten, Daten bei der Übertragung und Daten in Verarbeitung. Sie regelt zudem die für Backups, E-Mail, externe Datenübermittlungen und öffentlich erreichbare Websites eingesetzte Verschlüsselung.

3. Ziele

3.1 Sicherstellung, dass sensible und regulierte Daten jederzeit durch angemessene kryptografische Maßnahmen geschützt sind

3.2 Festlegung von Verantwortlichkeiten für die Auswahl, Konfiguration und Verwaltung von Verschlüsselungswerkzeugen und Schlüsseln

3.3 Verhinderung unbefugten Zugriffs, von Manipulationen oder Datenabfluss durch die Durchsetzung sicherer Kontrollen für Übertragung und Speicherung

3.4 Erfüllung gesetzlicher und regulatorischer Anforderungen, die die Verschlüsselung personenbezogener und geschäftlicher Daten vorschreiben

3.5 Aufrechterhaltung von Betriebssicherheit und Verfügbarkeit durch wirksame Verwaltung von Zertifikaten und kryptografischen Schlüsseln

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführung (GM)

4.1.1 genehmigt diese Richtlinie und stellt sicher, dass kryptografische Anforderungen durchgesetzt werden,

4.1.2 überprüft Ausnahmen, Meldungen zu Sicherheitsvorfällen und die Einhaltung von Verschlüsselungsklauseln durch Lieferanten,

4.1.3 verifiziert, dass ausgelagerte oder cloudbasierte Dienste die Verschlüsselungsstandards erfüllen.

4.2 IT-Support-Dienstleister / interner IT-Administrator

4.2.1 implementiert und betreibt Verschlüsselungslösungen (z. B. Festplattenvollverschlüsselung, TLS-Zertifikate, VPNs),

4.2.2 verwaltet die Lebenszyklen kryptografischer Schlüssel und Werkzeuge für die sichere Speicherung,

4.2.3 konfiguriert und überwacht die Verschlüsselung zum Schutz von Backups, Websites und Geräten.

[... 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 mindestens einmal jährlich durch die Geschäftsführung in Abstimmung mit dem IT-Support-Dienstleister und dem Datenschutzkoordinator überprüft werden.

9.2 Auslöser für eine außerplanmäßige Überprüfung

9.2.1 Überprüfungen müssen zusätzlich durchgeführt werden, wenn:

9.2.1.1 sich kryptografische Standards oder Protokolle ändern (z. B. Außerbetriebnahme eines Algorithmus),

9.2.1.2 neue Systeme oder Cloud-Dienste eingeführt werden,

9.2.1.3 eine Sicherheitsverletzung oder ein Vorfall einen kompromittierten Schlüssel oder ein kompromittiertes Zertifikat betrifft,

9.2.1.4 gesetzliche oder regulatorische Änderungen die Verschlüsselungsanforderungen beeinflussen.

9.3 Versionskontrolle und Kommunikation

9.3.1 Alle Änderungen an der Richtlinie müssen in einem Versionsprotokoll dokumentiert werden.

9.3.2 Das Personal muss über Aktualisierungen informiert werden, und frühere Versionen sind zu archivieren.

9.3.3 Die aktuell freigegebene Version muss im zentralen Richtlinien-Repository gespeichert werden.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie ist in Verbindung mit den folgenden SME-Richtlinien anzuwenden:

10.1.1 P12S – Richtlinie zum Asset-Management: Stellt sicher, dass Verschlüsselung bei klassifizierten Assets während der Speicherung, Übertragung und Entsorgung angewendet wird.

10.1.2 P14S – Richtlinie zur Datenaufbewahrung und Entsorgung: Definiert Aufbewahrungsfristen und verlangt die verschlüsselte Speicherung von Daten bis zu deren sicherer Löschung.

10.1.3 P17S – Richtlinie zu Datenschutz und Privatsphäre: Stimmt die Verschlüsselung mit Datenschutzgrundsätzen und regulatorischen Erwartungen nach Artikel 32 der DSGVO ab.

10.1.4 P22S – Richtlinie zur Protokollierung und Überwachung: Verlangt die Protokollierung der Schlüsselnutzung, von Verschlüsselungsfehlern und Zertifikatsabläufen für Audit-Zwecke.

10.1.5 P30S – Incident-Response-Richtlinie: Beschreibt Eskalations-, Eindämmungs- und Benachrichtigungsverfahren, wenn Verschlüsselung versagt oder Schlüssel kompromittiert werden.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 8.1 – Verlangt die Implementierung operativer Kontrollen, einschließlich Verschlüsselung, zur Steuerung von Sicherheitsrisiken.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 8.24 – Beschreibt Anforderungen an den Einsatz von Verschlüsselung zum Schutz von Vertraulichkeit und Integrität.

11.2.2 Maßnahme 8.25 – Beschreibt die sichere Verwaltung kryptografischer Schlüssel und Zertifikate.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Legt Anforderungen für die Einrichtung und Validierung kryptografischer Schlüssel fest.

11.3.2 SC-13 – Definiert Standards für die Generierung kryptografischer Schlüssel.

11.3.3 SC-17 – Umfasst Public Key Infrastructure (PKI) und die Verwaltung des Zertifikatslebenszyklus.

11.3.4 SC-28 – Verlangt die Verschlüsselung ruhender Daten.

11.3.5 SC-12 bis SC-17 (Familie) – Stellt sicher, dass kryptografische Schutzmaßnahmen systemübergreifend ordnungsgemäß umgesetzt werden.

11.4 EU DSGVO

11.4.1 Artikel 32(1)(a) – Verlangt von Organisationen die Umsetzung technischer Maßnahmen wie Verschlüsselung zur Sicherstellung der Vertraulichkeit von Daten.

11.4.2 Artikel 34 – Stellt klar, dass Verschlüsselung Organisationen von Meldepflichten bei Sicherheitsverletzungen befreien kann, wenn die Daten für Unbefugte unverständlich waren.

11.5 EU-NIS2-Richtlinie

11.5.1 Artikel 21(2)(d) – Verlangt wirksame Verschlüsselung zur Absicherung von Systemen und Kommunikation.

11.5.2 Artikel 21(2)(e) – Betont den Schutz von Daten und die Minderung von Cyberbedrohungen durch Verschlüsselung.

11.6 EU DORA

11.6.1 Artikel 6(2)(d) – Verlangt, dass IKT-Systeme sichere Kommunikationskanäle und Verschlüsselung aufrechterhalten.

11.6.2 Artikel 9(2)(f) – Verpflichtet Finanzunternehmen zum Einsatz starker Verschlüsselung zum Schutz digitaler Kommunikation und des Datenaustauschs.

11.7 COBIT 2019

11.7.1 DSS05.01 – Verlangt den Schutz sensibler Informationen durch Verschlüsselung und kryptografische Protokolle.

11.7.2 APO13.02 – Verlangt die wirksame Implementierung von Sicherheitskontrollen, einschließlich kryptografischer Schutzmaßnahmen, als Bestandteil der Sicherheitsplanung.