					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P18					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**

Abgleich mit Standards und regulatorischen Anforderungen

Standard/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 8	-
ISO/IEC 27002:2022	Maßnahmen 8.24, 8.25, 8	-
NIST SP 800-53 Rev. 5	SC-12 bis SC-17, SC-28, SC-28(1), SC-12(3)	-
EU-DSGVO	Artikel 32, Artikel 33–34, Erwägungsgrund 83	-
EU NIS2	Artikel 21(2)(d)	-
EU DORA	Artikel 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Zweck

1.1 Diese Richtlinie legt verbindliche Anforderungen für den sicheren und konformen Einsatz kryptografischer Kontrollen in der gesamten Organisation fest, um die Vertraulichkeit, Integrität und Authentizität sensibler und regulierter Informationen sicherzustellen.

1.2 Der Einsatz von Kryptografie bildet die Grundlage für vertrauenswürdige Datensicherheitsprozesse, unterstützt eine sichere Kommunikation, erzwingt Zugriffskontrollen und ermöglicht die Einhaltung regulatorischer Anforderungen durch wirksame Verschlüsselungs- und Schlüsselmanagementverfahren.

1.3 Diese Richtlinie steht im Einklang mit ISO/IEC 27001:2022, Klausel 8.1, und Anhang A, Maßnahme 8.24, und unterstützt rechtliche sowie operative Verpflichtungen nach Artikel 32 DSGVO, Artikel 6(2)(d) DORA und Artikel 21 NIS2. Zudem unterstützt sie die COBIT-2019-Ziele für Sicherheitsdienste und den Schutz von Informationswerten.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Organisationseinheiten, Geschäftsfunktionen, alle Beschäftigten sowie Drittanbieter, die am Einsatz, an der Administration oder an der Implementierung kryptografischer Werkzeuge und Verfahren beteiligt sind.

2.2 Erfasste Umgebungen umfassen Produktions-, Entwicklungs-, Staging-, Backup- und Disaster-Recovery-Systeme, in denen sensible Daten übertragen, verarbeitet oder gespeichert werden.

2.3 Der Geltungsbereich umfasst alle kryptografischen Komponenten und Anwendungsfälle, einschließlich, aber nicht beschränkt auf:

2.3.1 Symmetrische und asymmetrische Verschlüsselung

2.3.2 Digitale Signaturen und Zertifikate

2.3.3 Hash-Algorithmen

2.3.4 Sichere Schlüsselgenerierung, -verteilung und -vernichtung

2.3.5 Transport Layer Security (TLS), Festplattenvollverschlüsselung (FDE) und Verschlüsselung auf API-Ebene

2.3.6 Sichere Komponenten wie Hardware Security Modules (HSMs), Trusted Platform Modules (TPMs) und Key Management Systems (KMS)

2.4 Diese Richtlinie regelt den Einsatz von Kryptografie in Bezug auf:

2.4.1 Daten, die als Vertraulich, Hochvertraulich oder Reguliert klassifiziert sind

2.4.2 Authentifizierung und Prüfung digitaler Identitäten

2.4.3 Sichere Kommunikation mit externen Parteien

2.4.4 Schlüsselverwahrung und Dual-Control-Mechanismen

3. Ziele

3.1 Sicherstellen, dass kryptografische Technologien entsprechend dem Geschäftsrisiko, internationalen Standards und regulatorischen Vorgaben ausgewählt, genehmigt, implementiert und betrieben werden.

3.2 Etablierung einer standardisierten Governance-Struktur für die Verwaltung kryptografischer Dienste, einschließlich klarer Verantwortlichkeiten für Implementierung, Validierung und Ausnahmesteuerung.

3.3 Verhinderung der unbefugten Nutzung, fehlerhaften Konfiguration oder Überalterung kryptografischer Algorithmen und Kontrollen durch einen formalen Genehmigungs- und Überprüfungsprozess.

3.4 Sicherstellen, dass kryptografische Kontrollen in die Systementwurfsphase eingebettet und regelmäßig validiert werden, um Datenoffenlegung, Schlüsselk kompromittierung oder eine Schwächung von Protokollen zu verhindern.

3.5 Durchsetzung des Lebenszyklusmanagements für alle kryptografischen Schlüssel, einschließlich Generierung, Speicherung, Nutzung, Rotation, Widerruf und sicherer Vernichtung.

3.6 Einhaltung internationaler und regionaler Vorschriften, die Verschlüsselung und sichere Datenverarbeitung vorschreiben, einschließlich DSGVO, DORA, NIS2 und COBIT 2019.

4. Rollen und Verantwortlichkeiten

4.1 Informationssicherheitsmanager / CISO

4.1.1 Ist Eigentümer dieser Richtlinie und stellt deren Ausrichtung auf das Informationssicherheits-Managementsystem (ISMS) und auf ISO/IEC 27001 Anhang A, Maßnahme 8.24 sicher.

4.1.2 Genehmigt die Verwendung kryptografischer Algorithmen und Kontrollen und setzt deren Einhaltung organisationsweit durch.

4.2 Leiter Kryptografiebetrieb / Sicherheitsarchitekt

4.2.1 Verantwortet den täglichen Betrieb und die Administration kryptografischer Systeme.

4.2.2 Pflegt die Liste genehmigter kryptografischer Verfahren (Approved Cryptographic Methods List, ACML) und das Register für Schlüsselmanagement.

4.2.3 Führt Kryptografie-Designprüfungen (Cryptographic Design Reviews, CDRs) durch und bewertet neue kryptografische Technologien.

[... 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 jährlich durch den Informationssicherheitsmanager und den Leiter Kryptografiebetrieb zu überprüfen.

9.2 Auslöser für Überprüfungen sind unter anderem:

9.2.1 Die Entdeckung kryptografischer Schwachstellen (z. B. Algorithmus-Downgrade, Quantenangriffe)

9.2.2 Regulatorische Änderungen, die aktualisierte Verschlüsselungsstandards erfordern

9.2.3 Operative Feststellungen oder Auditfeststellungen, die Regelungslücken aufzeigen

9.2.4 Upgrades kryptografischer Werkzeuge oder Architekturänderungen

9.3 Aktualisierungen müssen versionskontrolliert im ISMS-Dokumentenlenkungsregister geführt und kommuniziert werden an:

9.3.1 Alle Administratoren mit kryptografischen Zugriffsrollen

9.3.2 Entwicklungsteams und DevSecOps-Verantwortliche

9.3.3 Drittanbieter mit vertraglichen Verpflichtungen zur Verschlüsselung

9.4 Das ISMS-Team muss sicherstellen, dass ersetzte Versionen archiviert und in Betriebsverfahren nicht mehr referenziert werden.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 P1 - Informationssicherheitsrichtlinie. Stellt die grundlegende Governance für alle Sicherheitsmaßnahmen bereit, einschließlich der Durchsetzung kryptografischer Kontrollen, des Schutzes von Informationswerten und sicherer Kommunikation.

10.2 P4 - Richtlinie zur Zugriffskontrolle. Stellt sicher, dass der logische Zugriff auf kryptografisches Material und Systeme zur Verwaltung von Verschlüsselung strikt auf Grundlage des Prinzips der minimalen Berechtigung und der Funktionstrennung beschränkt ist.

10.3 P6 - Risikomanagement-Richtlinie. Unterstützt die Bewertung von Risiken kryptografischer Kontrollen und dokumentiert die Risikobehandlungsstrategie für Ausnahmen, die Überalterung von Algorithmen oder Szenarien einer Schlüsselkompromittierung.

10.4 P12 - Richtlinie zum Asset-Management. Schreibt die Klassifizierung sensibler Daten und Hardware-Assets vor und bestimmt damit unmittelbar kryptografische Anforderungen und Verpflichtungen zur Schlüsselverwahrung.

10.5 P13 - Richtlinie zur Datenklassifizierung und Kennzeichnung. Definiert die Klassifizierungsstufen (z. B. Vertraulich, Reguliert), die spezifische Verschlüsselungsanforderungen bei der Übertragung und im Ruhezustand auslösen.

10.6 P14 - Richtlinie zur Datenaufbewahrung und Entsorgung. Legt Verfahren für die sichere Entsorgung verschlüsselter Speichermedien und kryptografischen Schlüsselmaterials am Ende des Lebenszyklus fest.

10.7 P30 - Incident-Response-Richtlinie. Beschreibt die Reaktionsstrategie der Organisation bei Schlüsselkompromittierung, missbräuchlicher Zertifikatsnutzung oder vermuteten algorithmischen Schwachstellen, einschließlich schnellem Widerruf und Meldung von Sicherheitsverletzungen.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 8.1 - Betriebliche Planung und Steuerung: Verlangt technische Sicherheitskontrollen, einschließlich kryptografischer Maßnahmen, als Teil operativer Schutzmaßnahmen.

11.2 ISO/IEC 27002:2022

11.2.1 Maßnahmen 8.24, 8.25, 8: Bietet Umsetzungshinweise zu Zielen kryptografischer Kontrollen, zur Auswahl von Algorithmen, zur Durchsetzung von Protokollen und zum Lebenszyklusmanagement von Zertifikaten.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 - Einrichtung kryptografischer Schlüssel: Stellt die sichere Generierung und den sicheren Austausch von Verschlüsselungsschlüsseln sicher. P18 definiert, wie symmetrische und asymmetrische Schlüssel unter Verwendung genehmigter Algorithmen und Protokolle generiert und ausgetauscht werden müssen.

11.3.2 SC-13 - Kryptografischer Schutz: Schreibt den Einsatz von Kryptografie zum Schutz der Vertraulichkeit und Integrität von Informationen vor. P18 schreibt Verschlüsselung für ruhende

Daten und Datenübertragungen auf Grundlage der Datenklassifizierung vor; die Algorithmusstandards sind an NIST FIPS 140-3 ausgerichtet.

11.3.3 SC-17 - Zertifikate der Public Key Infrastructure (PKI): Fordert die Implementierung einer PKI zur Unterstützung von Authentifizierung und digitalen Signaturen. P18 beschreibt den Einsatz der PKI zur Absicherung von Kommunikation, Systemidentitäten und administrativen Zugriffen.

11.3.4 SC-28, SC-28(1) - Schutz von Informationen im Ruhezustand und bei der Übertragung: Fordert die Verschlüsselung von Daten bei Speicherung oder Übertragung über nicht vertrauenswürdige Netzwerke. P18 schreibt die Durchsetzung von TLS, VPN-Tunneln, Festplattenvollverschlüsselung und sicheren Speichermethoden für sensible Daten vor.

11.3.5 SC-12(3) - Symmetrische Schlüsselgenerierung für sichere Speicherung und Verteilung: Konzentriert sich auf die sichere Generierung und Handhabung symmetrischer Schlüssel. P18 schreibt die Verwendung starker Zufallszahlengeneratoren, Vorgaben zur Schlüsselrotation und sicherer Schlüsselablagen für kryptografische Vorgänge vor.

11.4 EU-DSGVO (2016/679)

11.4.1 Artikel 32 - Sicherheit der Verarbeitung: Empfiehlt ausdrücklich Verschlüsselung als Maßnahme zur Risikoreduzierung für personenbezogene Daten.

11.4.2 Erwägungsgrund 83: Hebt Verschlüsselung als Kontrolle zur Verhinderung unbefugter Datenzugriffe hervor.

11.4.3 Artikel 33 und 34: Eine wirksame Verschlüsselung kann Organisationen von verpflichtenden Meldungen von Sicherheitsverletzungen ausnehmen.

11.5 EU NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(d): Fordert technische und organisatorische Maßnahmen, einschließlich kryptografischer Schutzmaßnahmen, zur Aufrechterhaltung der Verfügbarkeit und Integrität von Diensten.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 6(2)(d): Finanzinstitute müssen Daten absichern, auch durch starke Verschlüsselung kritischer Informationen.

11.6.2 Artikel 11(1)(c): Schreibt sichere Kontrollen der Datenverarbeitung für IKT-Drittdienstleister vor.

11.7 COBIT 2019

11.7.1 DSS05.01 - Informationswerte schützen: Fordert den Einsatz von Verschlüsselung und Schlüsselmanagement zum Schutz von Daten vor unbefugtem Zugriff.

11.7.2 DSS06.06 - Verwaltete Sicherheitstests: Empfiehlt die Validierung der Einhaltung kryptografischer Anforderungen als Teil von Schwachstellenbewertungen.

11.7.3 MEA03 - Überwachen, Evaluieren und Beurteilen der Compliance: Verlangt die kontinuierliche Sicherstellung der Wirksamkeit kryptografischer Kontrollen.