					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P27					Dokumenttitel: **Richtlinie zur Nutzung von Cloud-Diensten**							
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**

Ausgerichtet an Standards und Vorschriften

Standard/Verordnung	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 8	Anforderungen an die operative Planung und Steuerung in Cloud-Umgebungen.
ISO/IEC 27002:2022	Maßnahmen 5.23–5.25	Vorgaben zur Nutzung, Richtliniensteuerung und Sicherheit von Cloud-Services.
NIST SP 800-53 Rev. 5	AC-20, SA-9(5), SC-12–SC-28, SR-5	Nutzung externer Systeme, vertragliche und technische Anforderungen, kryptografische Schutzmaßnahmen, Schutz der Lieferkette.
DSGVO	Artikel 28, 32, Kapitel V	Anforderungen an Cloud-Auftragsverarbeiter, Sicherheit der Verarbeitung, Datenübermittlungen.
EU NIS2	Artikel 21(2)(f, i)	Anforderungen an Risiken durch Dritte und die Lieferkette.
EU DORA	Artikel 5(2), 28	Überwachung von IKT- und Drittparteienrisiken im Zusammenhang mit Cloud-Services für Finanzunternehmen.
COBIT 2019	BAI04, DSS01, DSS05	Verfügbarkeit von Cloud-Services, Betriebssteuerung und Sicherheitsmanagement.

1. Zweck

1.1 Diese Richtlinie legt die verbindlichen Anforderungen der Organisation für die sichere, regelkonforme und verantwortungsvolle Nutzung von Cloud-Computing-Services über die Bereitstellungsmodelle Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS) hinweg fest.

1.2 Ziel dieser Richtlinie ist es sicherzustellen, dass Cloud-Services so eingeführt und gesteuert werden, dass die Vertraulichkeit, Integrität und Verfügbarkeit von Informationswerten geschützt und zugleich regulatorische, rechtliche und vertragliche Verpflichtungen erfüllt werden.

1.3 Sie definiert Kontrollen zur Steuerung von Cloud-Risiken, zum Schutz von Daten, zur Überwachung der Compliance von Anbietern und zur Verhinderung nicht autorisierter Nutzung. Darüber hinaus unterstützt sie geschäftliche Innovation durch Cloud-Plattformen, indem sie Informationssicherheit, betriebliche Zuverlässigkeit und Kosteneffizienz in Einklang bringt.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer, externen Dienstleister und Berater, die im Auftrag der Organisation Cloud-Services bereitstellen, konfigurieren, darauf zugreifen, diese verwalten oder nutzen.

2.2 Sie gilt für alle Umgebungen, in denen Daten oder Workloads der Organisation verarbeitet werden, einschließlich:

2.2.1 Public-Cloud-, Private-Cloud-, Hybrid-Cloud- und Community-Cloud-Bereitstellungen

2.2.2 aller Cloud-Service-Modelle (IaaS, PaaS, SaaS)

2.2.3 Multi-Cloud- und föderierter Architekturen

2.2.4 der Nutzung von Shadow IT oder persönlichen Cloud-Konten für geschäftliche Zwecke

2.3 Sie umfasst alle Datenklassifizierungen und gilt sowohl für interne Systeme als auch für von Lieferanten gehostete Plattformen, auf denen organisationsinterne oder regulierte Daten gespeichert oder verarbeitet werden.

3. Ziele

3.1 Sicherstellung einer sicheren und konsistenten Nutzung von Cloud-Technologien durch klar definierte Nutzungsvorgaben, Sicherheitsbaselines und Governance-Rollen.

3.2 Minimierung betrieblicher und regulatorischer Risiken im Zusammenhang mit Cloud-Computing, einschließlich unbefugtem Zugriff, Datenschutzverletzungen, Fehlkonfigurationen, Nichteinhaltung und Dienstausfällen.

3.3 Durchsetzung von Sicherheits- und Datenschutzanforderungen für alle Cloud-Anbieter und Überprüfung der Einhaltung durch Vertragsklauseln, Bewertungen und Auditrechte.

3.4 Ermöglichung einer skalierbaren und resilienten Einführung von Cloud-Services, ohne das Informationssicherheitsrisiko, rechtliche Anforderungen oder die Aufrechterhaltung des Geschäftsbetriebs zu beeinträchtigen.

3.5 Ausrichtung der Cloud-Governance und -Nutzung am ISMS der Organisation, an rechtlichen Verpflichtungen (z. B. DSGVO, DORA), sektorspezifischen Vorgaben und branchenweit anerkannten Best Practices (z. B. NIST, COBIT).

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung

4.1.1 Genehmigt die Richtlinie zur Nutzung von Cloud-Diensten sowie die strategische Roadmap für die Einführung von Cloud-Services.

4.1.2 Prüft und genehmigt Ausnahmen mit hohem Risiko von den Standardanforderungen der Cloud-Governance.

4.1.3 Stellt sicher, dass Cloud-Initiativen angemessen finanziert, überwacht und in unternehmensweite Risikomanagementrahmen integriert werden.

4.2 Chief Information Security Officer (CISO)

4.2.1 Verantwortet diese Richtlinie sowie das organisationsweite Register für Cloud-Services.

4.2.2 Genehmigt die Aufnahme neuer Cloud-Anbieter auf Grundlage der Due Diligence und der Risikobewertung.

4.2.3 Prüft Nachweise zur Compliance der Anbieter und validiert die Ausrichtung an den Sicherheitsanforderungen.

[... 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 und bei Bedarf zu aktualisieren, um die fortlaufende Ausrichtung sicherzustellen an:

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

9.1.2 Änderungen der Normen ISO/IEC 27001 oder ISO/IEC 27002

9.1.3 Aktualisierungen der Cloud-Architektur, der Bedrohungslage oder des Serviceportfolios der Organisation

9.1.4 Vorfallsuntersuchungen, Auditergebnissen oder Erkenntnissen aus dem operativen Betrieb

9.2 Der CISO ist dafür verantwortlich, die Überprüfung einzuleiten und relevante Stakeholder einzuberufen, einschließlich:

9.2.1 Cloud-Sicherheitsarchitekt

9.2.2 Rechts- und Compliance-Team

9.2.3 Einkauf und Lieferantenmanager

9.2.4 Serviceverantwortliche und IT-Betrieb

9.3 Alle Aktualisierungen müssen:

9.3.1 versionskontrolliert und datiert sein

9.3.2 von der Geschäftsleitung genehmigt werden

9.3.3 den betroffenen Parteien, einschließlich Mitarbeitern, Auftragnehmern und Drittparteien, mitgeteilt werden

9.3.4 gemäß internen Dokumentationsrichtlinien archiviert werden

9.4 Zwischenprüfungen können ausgelöst werden durch:

9.4.1 neue Beauftragungen von CSPs oder wesentliche Migrationen

9.4.2 neu auftretende Bedrohungen für Cloud-Infrastrukturen

9.4.3 wesentliche Änderungen vertraglicher, rechtlicher oder sektorspezifischer Verpflichtungen

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie steht in engem Zusammenhang mit den folgenden internen Richtlinien und ist von ihnen abhängig:

10.1.1 P1 – Richtlinie zur Informationssicherheit: Legt die übergeordneten Grundsätze für den sicheren Betrieb von Systemen und Services fest, die diese Richtlinie im Cloud-Kontext konkretisiert.

10.1.2 P5 – Richtlinie zum Änderungsmanagement: Alle Änderungen an Cloud-Konfigurationen müssen den in P5 festgelegten Verfahren zur Änderungssteuerung folgen.

10.1.3 P13 – Richtlinie zur Datenklassifizierung und Kennzeichnung: Legt fest, wie Daten vor der Übertragung in die Cloud bewertet werden und wie Kontrollen wie Verschlüsselung und Datenresidenz anzuwenden sind.

10.1.4 P18 – Richtlinie zu kryptografischen Kontrollen: Gibt Standards für Verschlüsselung, Schlüsselmanagement und den Einsatz kryptografischer Algorithmen vor, die unmittelbar auf Konfigurationen von Cloud-Services anzuwenden sind.

10.1.5 P22 – Richtlinie zur Protokollierung und Überwachung: Legt Anforderungen an Protokollerfassung, Aufbewahrung und Analyse fest, die in Cloud-Umgebungen durchgesetzt werden müssen.

10.1.6 P30 – Incident-Response-Richtlinie: Definiert Verfahren für Eskalation, Eindämmung und Mängelbeseitigung bei cloudbezogenen Sicherheitsereignissen.

10.1.7 P33 – Richtlinie zur Audit- und Compliance-Überwachung: Unterstützt die Auditfähigkeit und die kontinuierliche Sicherstellung, dass Cloud-Kontrollen wirksam umgesetzt und überwacht werden.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001: Klausel 8.1 – Operative Planung und Steuerung: Verlangt von Organisationen die Umsetzung und Steuerung der Prozesse, die erforderlich sind, um Informationssicherheitsanforderungen zu erfüllen, einschließlich solcher für Cloud-Umgebungen.

11.2 ISO/IEC 27002:2022 – Maßnahmen 5.23 bis 5.25:

11.2.1 Anhang A Maßnahme 5.23 – Nutzung von Cloud-Services: Verlangt risikobasierte Bewertungen, formale Genehmigung und Dokumentation der Nutzung von Cloud-Services.

11.2.2 Anhang A Maßnahme 5.24 – Richtlinie zur Nutzung von Cloud-Services: Verlangt die Festlegung und Durchsetzung formaler Richtlinien zur Cloud-Nutzung, die an den organisatorischen Anforderungen und Risiken ausgerichtet sind.

11.2.3 Anhang A Maßnahme 5.25 – Sicherheit in Cloud-Services: Verlangt die Integration von Sicherheitsmaßnahmen, vertragliche Schutzvorkehrungen und die Überwachung cloudgehosteter Workloads und Daten.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 AC-20 – Nutzung externer Systeme: Verlangt definierte Regeln und Bedingungen für den Zugriff auf Ressourcen der Organisation von externen oder cloudbasierten Systemen aus.

11.3.2 SA-9(5) – Externe Informationssystemdienste: Verlangt vertragliche Sicherheitsanforderungen, Aufsicht und kontinuierliche Überwachung für Cloud-Systeme von Drittparteien.

11.3.3 SC-12 bis SC-28 – Kryptografische Schutzmaßnahmen, Schutz von Netzgrenzen und Integrität der Übertragung: Entsprechen den Anforderungen an Verschlüsselung, Identität und Zugriff für cloudbasierte Dienste sowie Daten bei der Übertragung.

11.3.4 SR-5 – Schutz der Lieferkette: Unterstützt die Prüfung und vertragliche Steuerung von CSPs, die an der Leistungserbringung beteiligt sind.

11.4 DSGVO (2016/679):

11.4.1 Artikel 28 – Pflichten des Auftragsverarbeiters: Verlangt formale Verträge mit Cloud-Anbietern, um Sicherheit, Vertraulichkeit und Auditierbarkeit der Verarbeitung personenbezogener Daten sicherzustellen.

11.4.2 Artikel 32 – Sicherheit der Verarbeitung: Unterstützt die Anwendung von Verschlüsselung, Zugriffskontrollen, Protokollierung und weiteren Schutzmaßnahmen in Cloud-Umgebungen.

11.4.3 Kapitel V – Internationale Datenübermittlungen: Verlangt die rechtmäßige Übermittlung von Daten außerhalb der EU/des EWR unter Verwendung von Schutzmaßnahmen wie SCCs oder Angemessenheitsbeschlüssen.

11.5 EU NIS2-Richtlinie (2022/2555):

11.5.1 Artikel 21(2)(f, i): Verlangt, dass Einrichtungen Risiken durch Drittanbieter von Cloud-Services steuern und die Integrität der digitalen Lieferkette durch vertragliche und technische Maßnahmen sicherstellen.

11.6 EU DORA (2022/2554):

11.6.1 Artikel 5(2) – Governance von IKT-Risiken: Verlangt die Integration von IKT-Drittparteienrisiken, einschließlich Cloud-Services, in die übergreifende Risiko-Governance.

11.6.2 Artikel 28 – Überwachung kritischer IKT-Drittanbieter: Verlangt von Finanzunternehmen, Abhängigkeiten von Cloud-Anbietern, deren Informationssicherheitsrisikoprofil und deren Resilienz zu überwachen, zu steuern und darüber Bericht zu erstatten.

11.7 COBIT 2019:

11.7.1 BAI04 – Verfügbarkeit und Kapazität verwalten: Stellt sicher, dass Cloud-Services resilient sind, überwacht werden und festgelegte Leistungskriterien erfüllen.

11.7.2 DSS01 – Betrieb verwalten: Unterstützt die operative Integration, die Behandlung von Sicherheitsvorfällen und Baseline-Konfigurationen über cloudgehostete Plattformen hinweg.

11.7.3 DSS05 – Sicherheitsdienste verwalten: Gibt die Umsetzung cloud-spezifischer Sicherheitskontrollen, Überwachung und Prävention von Sicherheitsvorfällen über digitale Dienste hinweg vor.