					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P27S					Dokumenttitel: **Richtlinie zur Nutzung von Cloud-Services**							
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/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 8	
ISO/IEC 27002:2022	Maßnahmen 5.23–5.25	
NIST SP 800-53 Rev. 5	AC-20, SC-12, SC-13, SR-5	
DSGVO	Artikel 28, 32 und Kapitel V	
EU-NIS2	Artikel 21(2)(f), (i)	
EU-DORA	Artikel 5(2), 28	
COBIT 2019	DSS01, DSS05, BAI04	

1. Zweck

1.1 Diese Richtlinie legt fest, wie Cloud-Services innerhalb der Organisation sicher genutzt werden dürfen. Sie stellt sicher, dass in der Cloud verarbeitete oder gespeicherte Daten geschützt, Zugriffe kontrolliert und Risiken angemessen gesteuert werden.

1.2 Sie unterstützt KMU dabei, gesetzliche Verpflichtungen und Kundenerwartungen zum Schutz sensibler Informationen, zur Vermeidung von Datenabfluss und zur wirksamen Steuerung cloudbezogener Risiken zu erfüllen, ohne eine Infrastruktur auf Unternehmensebene vorauszusetzen.

1.3 Diese Richtlinie unterstützt die Zertifizierung nach ISO/IEC 27001, die Einhaltung der DSGVO und die Absicherung der Lieferkette durch eine konsistente Governance aller Cloud-Services von Dritten.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 jeden cloudbasierten Dienst, der zum Speichern, Verarbeiten oder Übertragen von Unternehmensdaten verwendet wird

2.1.2 sämtliche Mitarbeitenden, Auftragnehmer oder Dienstleister, die Cloud-Werkzeuge im Namen der Organisation nutzen

2.1.3 kostenlose und kostenpflichtige Cloud-Lösungen, einschließlich E-Mail-Plattformen, Dokumentenfreigabe, SaaS-Werkzeuge, Backup-Plattformen, Videokonferenzlösungen und Kundenplattformen

2.1.4 jedes Gerät (Desktop-Computer, mobiles Gerät, Tablet), das über Cloud-Anwendungen auf Unternehmensinformationen zugreift

2.2 Dies umfasst unter anderem:

2.2.1 Microsoft 365, Google Workspace, Dropbox Business

2.2.2 Zoom, Microsoft Teams, Google Meet

2.2.3 AWS, Azure, GCP

2.2.4 cloudbasierte Werkzeuge für Backup und Disaster Recovery

2.2.5 gemeinsame Ordner oder Anwendungen, die für Rechnungsstellung, Projektmanagement oder Kundenkommunikation genutzt werden

3. Ziele

3.1 Die nicht autorisierte oder risikobehaftete Nutzung nicht genehmigter Cloud-Services verhindern.

3.2 Sicherstellen, dass sensible oder regulierte Daten, die in der Cloud gespeichert werden, durch angemessene technische und organisatorische Kontrollen geschützt sind.

3.3 Klare Rollen für die Genehmigung, Konfiguration, Überwachung und Außerbetriebnahme von Cloud-Services festlegen.

3.4 Datenflüsse steuern und Aufbewahrungs-, Lösch- und Datenschutzpflichten für in der Cloud gespeicherte Informationen durchsetzen.

3.5 Die Abhängigkeit von persönlichen Konten oder nicht nachverfolgten Werkzeugen reduzieren, indem für alle geschäftlich genutzten Cloud-Systeme eine Genehmigung vorgeschrieben wird.

3.6 Die Anforderungen aus ISO/IEC 27001:2022, DSGVO, NIS2 und DORA für die Steuerung externer Cloud-Abhängigkeiten einhalten.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführung (GM)

4.1.1 genehmigt die Nutzung aller neuen Cloud-Services

4.1.2 bewertet Risiken im Zusammenhang mit Cloud-Anbietern und Servicearten

4.1.3 setzt diese Richtlinie durch und beaufsichtigt Entscheidungen über Ausnahmen

4.2 IT-Dienstleister oder technischer Support

4.2.1 bewertet und implementiert sichere Konfigurationen für Cloud-Services

4.2.2 richtet Konten, Zugriffskontrollen und Backups ein

4.2.3 überwacht die Einhaltung von Passwortvorgaben, Multi-Faktor-Authentifizierung und Sicherheitseinstellungen

[... 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 durch die Geschäftsführung in Abstimmung mit dem IT-Dienstleister zu überprüfen.

9.2 Eine formale Überprüfung muss außerdem erfolgen:

9.2.1 nach einem cloudbezogenen Informationssicherheitsvorfall (z. B. Sicherheitsverletzung, Datenverlust)

9.2.2 wenn eine neue wesentliche Cloud-Plattform eingeführt wird

9.2.3 wenn sich gesetzliche oder regulatorische Anforderungen ändern (z. B. Aktualisierungen der DSGVO, NIS2 oder DORA)

9.2.4 wenn Überwachungstätigkeiten Missbrauch oder neue Risiken aufdecken

9.3 Die Geschäftsführung muss sicherstellen, dass:

9.3.1 das Register für Cloud-Services mit neuen oder außer Betrieb genommenen Diensten aktualisiert wird

9.3.2 rechtliche Anforderungen und Datenschutzanforderungen weiterhin erfüllt werden

9.3.3 alle Änderungen den relevanten Benutzern und Interessenträgern kommuniziert werden

9.4 Archivierte Versionen sind sicher aufzubewahren, und frühere Richtlinienversionen sind gemäß der P14S – Richtlinie zur Datenaufbewahrung und Entsorgung der Organisation zu behandeln.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie ist in Verbindung mit den folgenden auf KMU ausgerichteten Richtlinien zur Informationssicherheit anzuwenden:

10.1.1 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Definiert die Rechenschaftspflicht für die Genehmigung von Cloud-Services und die Steuerung von Anbieterbeziehungen.

10.1.2 P4S – Richtlinie zur Zugriffskontrolle: Unterstützt sichere Anmelde-, Sitzungsverwaltungs- und Entzugspraktiken, die für Cloud-Plattformen erforderlich sind.

10.1.3 P14S – Richtlinie zur Datenaufbewahrung und Entsorgung: Regelt, wie cloudbasierte Daten in Übereinstimmung mit gesetzlichen Verpflichtungen gesichert, aufbewahrt und gelöscht werden.

10.1.4 P17S – Richtlinie zu Datenschutz und Privatsphäre: Stellt sicher, dass in Cloud-Services gespeicherte personenbezogene Daten gemäß den Grundsätzen der DSGVO verarbeitet werden.

10.1.5 P30S – Richtlinie für Incident Response: Enthält strukturierte Verfahren zur Reaktion auf Cloud-Sicherheitsvorfälle, einschließlich Beweissicherung und externer Benachrichtigung.

10.2 Zusammen stellen diese Richtlinien sicher, dass die Cloud-Nutzung sicher, regelkonform und betrieblich resilient ist.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 8.1 – verlangt von Organisationen die Umsetzung operativer Kontrollen für die Datenverarbeitung, einschließlich solcher im Zusammenhang mit cloudbasierten Systemen.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 5.23 – verlangt Governance über die Nutzung von Cloud-Services und SaaS-Werkzeugen von Dritten.

11.2.2 Maßnahme 5.24 – verlangt eine definierte Richtlinie zur Cloud-Nutzung, die auf Risiken und regulatorische Anforderungen abgestimmt ist.

11.2.3 Maßnahme 5.25 – verlangt von Organisationen sicherzustellen, dass Sicherheitskontrollen in Cloud-Umgebungen den organisatorischen Anforderungen entsprechen.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-20 – verlangt formale Nutzungsrichtlinien für externe Systeme wie Cloud-Services.

11.3.2 SC-12, SC-13 – behandeln Verschlüsselung für Daten während der Übertragung und im Ruhezustand in Cloud-Umgebungen.

11.3.3 SR-5 – behandelt Kontrollen zu Cloud- und Drittparteienrisiken innerhalb der Lieferkette.

11.4 DSGVO (2016/679)

11.4.1 Artikel 28 – verlangt, dass Cloud-Anbieter, die als Auftragsverarbeiter handeln, verbindliche vertragliche Verpflichtungen einhalten.

11.4.2 Artikel 32 – verlangt technische und organisatorische Maßnahmen für die cloudbasierte Verarbeitung von Daten.

11.4.3 Kapitel V – untersagt nicht autorisierte internationale Übermittlungen personenbezogener Daten, die in der Cloud gespeichert sind.

11.5 EU-NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(f), (i) – verlangt von wesentlichen und wichtigen Einrichtungen die Umsetzung angemessener Richtlinien zur Sicherheit von Cloud-Services und zur Steuerung der Lieferkette.

11.6 EU-DORA (2022/2554)

11.6.1 Artikel 5(2) – verlangt von Finanz-KMU, Cloud-Sicherheit in ihre Rahmenwerke für das Management von IKT-Risiken zu integrieren.

11.6.2 Artikel 28 – legt Aufsichtsregeln für kritische IKT-Drittdienstleister fest, einschließlich Cloud-Anbietern.

11.7 COBIT 2019

11.7.1 DSS01 – „Manage Operations“ behandelt die operative Integrität von Cloud-Services.

11.7.2 DSS05 – „Manage Security Services“ umfasst cloudspezifische Schutzmaßnahmen und Überwachung.

11.7.3 BAI04 – „Manage Availability and Capacity“ stellt die Aufrechterhaltung des Geschäftsbetriebs und der Leistung in Cloud-Umgebungen sicher.