					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P15S					Dokumenttitel: **Richtlinie für Backup und Wiederherstellung**							
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 regulatorischen Anforderungen

Standard/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 8	Backup-Kontrollen gemäß den Anforderungen des Informationssicherheitsmanagementsystems (ISMS)
ISO/IEC 27002:2022	Maßnahmen 5.29, 8.13	Bewährte Verfahren für Backups und deren Einbindung in die Aufrechterhaltung des Geschäftsbetriebs
NIST SP 800-53 Rev. 5	CP-9, MP-6	Backup und Schutz von Speichermedien
EU-NIS2-Richtlinie	Artikel 21(2)(c)	Resilienz und Kontinuität durch Backups
EU DORA	Artikel 10(1)	IKT-Kontinuität – Backups für Finanzunternehmen
COBIT 2019	BAI04.05, DSS04	Dokumentation und Test von Backups sowie Steuerung der Prozesse
DSGVO	Artikel 5(1)(f), 32(1)(c)	Integrität, Verfügbarkeit und zeitnahe Wiederherstellung von Daten

1. Zweck

1.1 Diese Richtlinie legt fest, wie die Organisation Backups durchführt und verwaltet, um die Aufrechterhaltung des Geschäftsbetriebs sicherzustellen, vor Datenverlust zu schützen und eine zeitnahe Wiederherstellung nach Vorfällen zu ermöglichen.

1.2 Sie definiert verbindliche Vorgaben dazu, wie Systeme und Daten gesichert, gespeichert und wiederhergestellt werden müssen, insbesondere in KMU ohne komplexe IT-Infrastruktur.

1.3 Diese Richtlinie unterstützt die Auditfähigkeit und die Zertifizierung nach ISO/IEC 27001, indem sichergestellt wird, dass wesentliche Backup-Kontrollen vorhanden sind, einheitlich angewendet und regelmäßig überprüft werden.

1.4 Die Fähigkeit der Organisation, sich von technischen Ausfällen, versehentlichem Löschen oder Cyberangriffen zu erholen, hängt von der konsequenten Einhaltung dieser Richtlinie ab.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Geschäftssysteme und Daten, einschließlich:

2.1.1 Finanzunterlagen, Kundeninformationen und Personaldaten

2.1.2 Desktop-PCs, Laptops, Server und Cloud-Anwendungen, die im Geschäftsbetrieb genutzt werden

2.1.3 Backup-Medien wie USB-Laufwerke, externe Speichermedien oder Cloud-basierte Backups

2.2 Sie gilt außerdem für alle Personen, die für die Durchführung oder Verwaltung von Backup-Prozessen verantwortlich sind, einschließlich:

2.2.1 der Geschäftsleitung oder einer benannten verantwortlichen Person

2.2.2 externer IT-Dienstleister oder Berater

2.2.3 aller Mitarbeitenden, die dafür verantwortlich sind, Daten an genehmigten Speicherorten zu speichern

3. Ziele

3.1 Sicherstellen, dass alle kritischen Geschäftsdaten und Systeme auf Grundlage des Risikos und der betrieblichen Erfordernisse in geeigneten Intervallen zuverlässig gesichert werden.

3.2 Gewährleisten, dass Daten nach Störungen zeitnah und vollständig wiederhergestellt werden können.

3.3 Verhindern, dass Unbefugte auf Backup-Daten zugreifen, diese manipulieren oder dass sie durch wirksame Speicherkontrollen verloren gehen.

3.4 Rollen und Verantwortlichkeiten für die Umsetzung und Überprüfung von Backup-Verfahren klar festlegen und durchsetzen.

3.5 Die Einhaltung von ISO/IEC 27001, DSGVO und anderen regulatorischen Verpflichtungen durch strukturierte und dokumentierte Backup-Praktiken unterstützen.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung

4.1.1 genehmigt diese Richtlinie und stellt ihre Durchsetzung sicher

4.1.2 weist Ressourcen zu und benennt die Verantwortlichen für Backup- und Wiederherstellungsaktivitäten

4.1.3 prüft Backup-Fehler, Vorfälle oder Abweichungen von dieser Richtlinie

4.1.4 veranlasst die jährliche Überprüfung der Richtlinie und stellt die Auditfähigkeit sicher

4.2 IT-Support-Dienstleister (falls zutreffend)

4.2.1 implementiert und verwaltet Backup-Lösungen (lokal oder cloudbasiert)

4.2.2 überwacht den Erfolg der Backups und plant Wiederherstellungstests

4.2.3 meldet Fehler und Vorfälle unmittelbar an die Geschäftsleitung

4.2.4 stellt Verschlüsselung, Zugriffsbeschränkungen und den ordnungsgemäßen Umgang mit Backup-Medien sicher

[... 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 muss mindestens einmal jährlich durch die Geschäftsleitung überprüft werden. Auslöser für außerplanmäßige Überprüfungen sind:

9.1.1 wesentliche Änderungen an Systemen oder Speichermethoden

9.1.2 die Einführung neuer Cloud- oder IT-Plattformen

9.1.3 rechtliche oder regulatorische Änderungen, die sich auf die Datenwiederherstellung auswirken

9.1.4 Feststellungen aus Audits oder Vorfällen

9.2 Die Geschäftsleitung ist dafür verantwortlich, die Überprüfung einzuleiten, Änderungen zu genehmigen und Aktualisierungen zu kommunizieren.

9.3 Richtlinienversionen müssen nachvollziehbar versioniert und archiviert werden. Ersetzte Versionen müssen zugriffsbeschränkt werden, um Verwechslungen bei Audits oder Wiederherstellungsvorgängen im Geschäftsbetrieb zu vermeiden.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie ist mit den folgenden SME-Richtlinien abgestimmt und von ihnen abhängig:

10.1.1 P14S – Richtlinie zur Datenaufbewahrung und Entsorgung: Legt fest, wie lange Backup-Daten aufbewahrt und sicher gelöscht werden müssen.

10.1.2 P13S – Richtlinie zur Datenklassifizierung und Kennzeichnung: Unterstützt die Priorisierung der Daten, die anhand ihrer Klassifizierungsstufe gesichert werden müssen.

10.1.3 P30S – Incident-Response-Richtlinie: Regelt Verfahren für den Fall, dass Backups fehlschlagen oder nach einer Sicherheitsverletzung oder einem Ausfall eine Datenwiederherstellung erforderlich ist.

10.1.4 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Weist klare Zuständigkeiten für die Backup-Aufsicht und die Durchsetzung der Richtlinie zu.

10.1.5 P17S – Richtlinie zu Datenschutz und Privatsphäre: Stellt sicher, dass der Umgang mit personenbezogenen Daten in Backups mit rechtlichen und datenschutzbezogenen Anforderungen im Einklang steht.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 8.1: Operative Planung und Steuerung von Backup-Systemen als Teil des Informationssicherheitsmanagementsystems

11.2 ISO/IEC 27002

11.2.1 Maßnahme 8.13: Legt bewährte Verfahren für Backup-Planung, Überwachung und Wiederherstellung fest

11.2.2 Anhang A Maßnahme 5.29: Integration von Backups in die Aufrechterhaltung des Geschäftsbetriebs und Wiederherstellungsbereitschaft

11.3 NIST SP 800-53 Rev. 5

11.3.1 CP-9 (Notfallplanung): Definiert strukturierte Backup-Strategien für die Resilienz des Geschäftsbetriebs

11.3.2 MP-6 (Schutz von Speichermedien): Verlangt den sicheren Umgang mit und die sichere Vernichtung von Backup-Medien

11.4 DSGVO

11.4.1 Artikel 5(1)(f): Verlangt Integrität und Verfügbarkeit personenbezogener Daten

11.4.2 Artikel 32(1)(c): Verlangt die Fähigkeit, den Zugriff auf personenbezogene Daten zeitnah wiederherzustellen

11.5 EU-NIS2-Richtlinie

11.5.1 Artikel 21(2)(c): Verlangt Backup und Wiederherstellung als Teil der Resilienz- und Kontinuitätsplanung

11.6 EU DORA

11.6.1 Artikel 10(1): Organisationen des Finanzsektors müssen Backups als Teil von Maßnahmen zur IKT-Kontinuität sicherstellen

11.7 COBIT 2019

11.7.1 BAI04.05: Verlangt dokumentierte Backup-Strategien

11.7.2 DSS04.07: Betont routinemäßige Tests und Kontrollen für Daten-Backup- und Wiederherstellungsprozesse