					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P32S					Dokumenttitel: **Richtlinie zur Aufrechterhaltung des Geschäftsbetriebs und Disaster Recovery**							
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	Klauseln 6.1, 6.3, 8	
ISO/IEC 27002:2022	Maßnahmen 5.29, 5	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
EU-DSGVO	Artikel 32, 33	
EU-NIS2	Artikel 21(2)(f)	
EU-DORA	Artikel 10	
COBIT 2019	DSS	

1. Zweck

1.1 Diese Richtlinie stellt sicher, dass die Organisation in der Lage ist, den Geschäftsbetrieb aufrechtzuerhalten und wesentliche IT-Services während und nach Störungen wie Stromausfällen, Cyberangriffen, Ransomware-Infektionen oder Systemausfällen wiederherzustellen.

1.2 Sie legt einen klaren Rahmen für die Planung zur Aufrechterhaltung des Geschäftsbetriebs und für Disaster Recovery (BC/DR) fest, der auf KMU ohne dedizierte IT-Teams zugeschnitten ist.

1.3 Diese Richtlinie unterstützt die Organisation dabei, einschlägige Anforderungen nach ISO/IEC 27001:2022, DSGVO, NIS2, DORA und COBIT 2019 zu erfüllen und zugleich die betriebliche Resilienz sowie das Vertrauen der Kunden zu stärken.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle geschäftskritischen Systeme und Services (z. B. E-Mail, Cloud-Speicher, Rechnungsplattformen, Kundendatensätze)

2.1.2 alle Mitarbeitenden, Auftragnehmer und externen IT-Dienstleister, die für die BC/DR-Bereitschaft und -Umsetzung verantwortlich sind

2.1.3 alle Arten von Störungen, einschließlich Cybervorfällen, Hardwareausfällen, Stromausfällen, Überflutungen und der Unzugänglichkeit von Bürostandorten

2.2 Sie umfasst:

2.2.1 Backup-Management

2.2.2 Planung zur Aufrechterhaltung des Geschäftsbetriebs (BCP)

2.2.3 Disaster-Recovery-Verfahren

2.2.4 Schulung des Personals sowie Tests und Validierung

2.2.5 rechtliche und regulatorische Reaktionsverfahren

3. Ziele

3.1 Schutz der Fähigkeit der Organisation, zentrale Services trotz ungeplanter Störungen bereitzustellen.

3.2 Sicherstellung der zeitgerechten Wiederherstellung von Systemen und Daten anhand vordefinierter Wiederherstellungszeitziele (RTOs).

3.3 Sicherstellung, dass sämtliches Personal Kontinuitätsverfahren in Krisensituationen mit minimaler Unsicherheit befolgen kann.

3.4 Aufrechterhaltung der Einhaltung gesetzlicher und regulatorischer Anforderungen an Datenschutz und betriebliche Resilienz, einschließlich Artikel 32 DSGVO und Artikel 21 NIS2.

3.5 Etablierung einer praktikablen und testbaren Strategie zur Aufrechterhaltung des Geschäftsbetriebs und zur Wiederherstellung, die für KMU geeignet ist.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführung (GM)

4.1.1 trägt die Gesamtverantwortung für den BC/DR-Prozess und diese Richtlinie

4.1.2 genehmigt den Business-Continuity-Plan (BCP)

4.1.3 koordiniert die Reaktion auf Vorfälle und die interne Kommunikation während Störungen

4.1.4 veranlasst erforderliche regulatorische Meldungen (z. B. Meldungen von Datenschutzverletzungen nach DSGVO)

4.2 IT-Support-Dienstleister / Systemadministrator

4.2.1 verwaltet und testet Backups

4.2.2 führt im Auslösefall die Disaster-Recovery-Verfahren aus

4.2.3 dokumentiert sämtliche Wiederherstellungsmaßnahmen und Ereignisse der Systemwiederherstellung

4.2.4 meldet kritische IT-Vorfälle unverzüglich an die Geschäftsführung

[... 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 von Richtlinie und Plan

9.1.1 Die Geschäftsführung (GM) muss sicherstellen, dass diese Richtlinie und der zugehörige Business-Continuity-Plan (BCP) mindestens einmal jährlich formell überprüft werden.

9.1.2 Die Überprüfung muss Folgendes umfassen:

9.1.2.1 Bewertung neuer oder neu entstehender Risiken

9.1.2.2 Revalidierung der RTOs/RPOs

9.1.2.3 Verifizierung von Lieferanten- und Kontaktinformationen

9.1.2.4 Ausrichtung an Änderungen in IT-Systemen, rechtlichen Verpflichtungen oder Betriebsabläufen

9.2 Anlassbezogene Aktualisierungen

9.2.1 Diese Richtlinie muss außerdem als Reaktion auf Folgendes aktualisiert werden:

9.2.1.1 wesentliche Vorfälle oder Störungen, insbesondere wenn Ziele nicht erreicht wurden

9.2.1.2 neue gesetzliche oder regulatorische Verpflichtungen (z. B. Änderungen an DORA)

9.2.1.3 Änderungen an kritischen Systemen, Cloud-Plattformen oder beim Personal

9.2.1.4 Feststellungen aus jährlichen BCP/DR-Tests

9.3 Änderungssteuerungsprozess

9.3.1 Alle Änderungen müssen von der Geschäftsführung genehmigt werden

9.3.2 Es muss ein Versionsprotokoll geführt werden, einschließlich Datum, Beschreibung der Änderung und Genehmigendem

9.3.3 Die aktualisierte Richtlinie muss an sämtliches relevantes Personal erneut verteilt werden, einschließlich des IT-Support-Dienstleisters und der Abteilungsleiter

9.4 Dokumentation gewonnener Erkenntnisse

9.4.1 Nach Tests oder tatsächlichen Störungen müssen dokumentierte gewonnene Erkenntnisse in künftige Überarbeitungen einfließen

9.4.2 Diese Überprüfungen müssen außerdem Bewertungen der Lieferantenleistung und Prüfungen der Angemessenheit der Reaktion umfassen

10. Verwandte Richtlinien und Verknüpfungen

10.1 Diese Richtlinie ist eng mit den folgenden SME-Richtlinien verknüpft:

10.1.1 P1S – Informationssicherheitsrichtlinie: Definiert die übergeordneten Sicherheitsziele, die durch Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs und Wiederherstellung unterstützt werden müssen.

10.1.2 P4S – Richtlinie zur Zugriffskontrolle: Ermöglicht den Notfallentzug oder die Wiederherstellung von Benutzerzugriffen in Szenarien mit Geschäftsunterbrechungen.

10.1.3 P6S – Risikomanagement-Richtlinie: Bildet die Grundlage für die Identifizierung, Risikobewertung und Priorisierung von Risiken im Zusammenhang mit der Aufrechterhaltung des Geschäftsbetriebs.

10.1.4 P8S – Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit: Stellt sicher, dass Mitarbeitende darauf vorbereitet sind, während Störungen zu handeln, und den BCP verstehen.

10.1.5 P15S – Richtlinie für Backup und Wiederherstellung: Legt spezifische technische Verfahren zum Schutz der Datenverfügbarkeit und zur Wiederherstellung fest.

10.1.6 P17S – Richtlinie zu Datenschutz und Privatsphäre: Stellt sicher, dass die Planung zur Aufrechterhaltung des Geschäftsbetriebs den Schutz personenbezogener Daten berücksichtigt und während und nach Vorfällen mit der DSGVO im Einklang steht.

10.1.7 P22S – Richtlinie zur Protokollierung und Überwachung: Unterstützt die Erkennung von Ereignissen, die BC/DR-Prozesse auslösen können, und stellt nach Störungen forensische Prüfpfade bereit.

10.1.8 P30S – Incident-Response-Richtlinie (P30): Geht der Aktivierung des Wiederherstellungsprozesses bei Cybervorfällen oder betrieblichen Vorfällen unmittelbar voraus.

10.1.9 P31S – Richtlinie zur Beweissicherung und Forensik: Stellt sicher, dass digitale Nachweise während Kontinuitätsszenarien für Compliance, Versicherungszwecke oder Untersuchungen erfasst werden.

10.2 Diese Richtlinien bilden zusammen ein kohärentes, auditbereites Rahmenwerk für Resilienz, Rechenschaftspflicht und die Aufrechterhaltung von Kontrollen über alle SME-Betriebsabläufe hinweg.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001:

11.1.1 Klausel 6.1 – fordert risikobasierte Planung und Risikobehandlung, einschließlich Aufrechterhaltung des Geschäftsbetriebs und Wiederherstellung.

11.1.2 Klausel 6.3 – betont die kontinuierliche Verbesserung nach Störungen.

11.1.3 Klausel 8.1 – schreibt betriebliche Kontrollen vor, einschließlich dokumentierter Kontinuitätsmaßnahmen.

11.2 ISO/IEC 27002:

11.2.1 Maßnahme 5.29 – fordert die Einrichtung und Aufrechterhaltung von Vorkehrungen zur Aufrechterhaltung des Geschäftsbetriebs.

11.2.2 Maßnahme 5.30 – fordert Tests und Überprüfungen dieser Vorkehrungen.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – definiert Anforderungen an die Notfallplanung.

11.3.2 CP-4 – schreibt Schulungen zur Notfallvorsorge für das Personal der Organisation vor.

11.3.3 CP-6 – behandelt Anforderungen an alternative Speicherstandorte.

11.3.4 CP-7 – regelt Erwartungen an alternative Verarbeitungsstandorte.

11.4 EU-DSGVO:

11.4.1 Artikel 32 – fordert Maßnahmen zur Gewährleistung der fortlaufenden Verfügbarkeit und Resilienz von Verarbeitungssystemen und -diensten.

11.4.2 Artikel 33 – löst Meldepflichten bei Datenschutzverletzungen aus, wenn eine Kontinuitätsstörung zur Kompromittierung personenbezogener Daten führt.

11.5 EU-NIS2-Richtlinie (2022/2555):

11.5.1 Artikel 21(2)(f) – fordert die Planung zur Aufrechterhaltung des Geschäftsbetriebs und Krisenmanagementfähigkeiten als Voraussetzung für die Bereitschaft im Cyberrisikomanagement.

11.6 EU-DORA-Verordnung (2022/2554):

11.6.1 Artikel 10 – schreibt die Durchführung von Tests zur digitalen operationalen Resilienz und Wiederherstellungsfähigkeiten vor, insbesondere für KMU im Finanzsektor.

11.7 COBIT 2019:

11.7.1 DSS04 – Manage Continuity: Bietet Leitlinien der Unternehmensführung zur Aufrechterhaltung und Validierung der betrieblichen Resilienz, einschließlich Verantwortlichkeit, Tests, Lieferantenintegration und Überprüfungen nach Ereignissen.