					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P32					Dokumenttitel: **Richtlinie zur Aufrechterhaltung des Geschäftsbetriebs und zur Notfallwiederherstellung**							
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 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1 bis CP-11	
NIST SP 800-34 Rev.1	Notfallplanung	Rahmenwerk
ISO 22301:2019		Anforderungen an Business-Continuity-Managementsysteme
EU-DSGVO	Artikel 32	
EU NIS2	Artikel 21(2)(f)	
EU DORA	Artikel 10	
COBIT 2019	DSS04	

1. Zweck

1.1. Diese Richtlinie legt die verbindlichen Kontrollen und Verantwortlichkeiten fest, um sicherzustellen, dass die Organisation kritische Geschäftsprozesse und unterstützende IKT-Services während und nach einem Störfall aufrechterhalten oder wiederherstellen kann.

1.2. Sie dient dem Schutz von Leben, der betrieblichen Stabilität, der Einhaltung rechtlicher Verpflichtungen, der Erfüllung von Kundenanforderungen und dem Schutz des Rufs der Organisation, indem Resilienz durch vorausschauende Planung und validierte Wiederherstellungsfähigkeiten verankert wird.

1.3. Diese Richtlinie bildet die Grundlage für das organisationsweite Rahmenwerk zur Aufrechterhaltung des Geschäftsbetriebs und zur Notfallwiederherstellung und stellt die Einhaltung geltender regulatorischer, vertraglicher und branchenspezifischer Anforderungen sicher.

2. Geltungsbereich

2.1. Diese Richtlinie gilt für alle Organisationseinheiten, Informationssysteme, Geschäftsprozesse, Mitarbeitenden sowie Services von Drittparteien, die auf Grundlage der Ergebnisse der Business Impact Analysis (BIA) als kritisch oder wesentlich eingestuft sind.

2.2. Die Richtlinie umfasst:

2.2.1. natürliche und vom Menschen verursachte Störungen, einschließlich Cyberangriffe, Infrastrukturausfälle, Ausfälle von Rechenzentren, Pandemien und Unterbrechungen von Lieferantenservices

2.2.2. Planung, Tests und kontinuierliche Verbesserung von Business-Continuity-Plänen (BCPs) und Disaster-Recovery-Plänen (DRPs)

2.2.3. Rollen und Verantwortlichkeiten für Notfallreaktion, Wiederherstellungskoordination und Vorfalleskalation

2.3. Sämtliche Mitarbeitenden mit Verantwortlichkeiten für Kontinuität oder Wiederherstellung, einschließlich IT, Prozessverantwortliche, Krisenmanager und Lieferanten, unterliegen den Bestimmungen dieser Richtlinie.

3. Ziele

3.1. Sicherstellung der Aufrechterhaltung des Geschäftsbetriebs und der Services durch vordefinierte und getestete Verfahren, um betriebliche, reputationsbezogene und rechtliche Auswirkungen zu minimieren.

3.2. Wiederherstellung von IKT-Services innerhalb definierter Recovery Time Objectives (RTOs) und Recovery Point Objectives (RPOs), ausgerichtet an der geschäftlichen Risikotoleranz.

3.3. Festlegung eindeutiger Verantwortlichkeiten für Planung, Umsetzung und Governance der Aufrechterhaltung des Geschäftsbetriebs und der Notfallwiederherstellung im gesamten Unternehmen.

3.4. Sicherstellung, dass Kontinuitätsfähigkeiten regelmäßig getestet, gepflegt und auf Grundlage realistischer Szenarien und Audit-Feststellungen verbessert werden.

3.5. Erfüllung der Compliance-Verpflichtungen aus ISO, NIST, DSGVO, DORA und NIS2 zur Unterstützung der gebotenen Sorgfalt im Hinblick auf operationelle Resilienz und Verfügbarkeit.

4. Rollen und Verantwortlichkeiten

4.1. Geschäftsleitung

4.1.1. Genehmigt die Richtlinie zur Aufrechterhaltung des Geschäftsbetriebs und zur Notfallwiederherstellung und stellt die strategische Ausrichtung sicher.

4.1.2. Stellt Budget und Ressourcen für die Aufrechterhaltung des Geschäftsbetriebs, die Notfallreaktion und Wiederherstellungsübungen bereit.

4.2. Business-Continuity-Manager

4.2.1. Verantwortet die Entwicklung und Pflege organisationsweiter Business-Continuity-Pläne sowie die Koordination von Kontinuitätstests.

4.2.2. Pflegt den BIA-Zeitplan, koordiniert Schulungen und stellt sicher, dass die Dokumentation den Compliance-Anforderungen entspricht.

[... 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 jährlich durch den Business-Continuity-Manager und den CISO überprüft werden, um die Ausrichtung auf Folgendes sicherzustellen:

9.1.1. Änderungen im Geschäftsbetrieb, an kritischen Systemen oder in der Infrastruktur

9.1.2. Erkenntnisse aus Vorfällen, Audits, Tabletop-Übungen oder DR-Tests

9.1.3. aktualisierte regulatorische oder vertragliche Verpflichtungen (z. B. DORA, DSGVO, Kundenanforderungen an RTO/RPO)

9.1.4. Änderungen der organisatorischen Risikobereitschaft oder Kontinuitätsstrategie

9.2. Die Überprüfungen müssen Folgendes umfassen:

9.2.1. Validierung der Relevanz der Pläne und der Kontaktdaten

9.2.2. Neubewertung von RTOs, RPOs und der Wiederherstellungsklassifizierung

9.2.3. Bewertung der Kapazität von Backup- und DR-Services

9.2.4. Rückmeldungen von Interessenträgern, die kürzlich Wiederherstellungspläne umgesetzt oder Tests durchgeführt haben

9.3. Alle Änderungen an der Richtlinie müssen:

9.3.1. versionskontrolliert mit dokumentierter Begründung und Freigabe durch die relevanten Interessenträger erfolgen

9.3.2. an Schlüsselpersonal und Teams mit aktualisierten Verantwortlichkeiten kommuniziert werden

9.3.3. in aktualisierten Schulungen, Sensibilisierungsmaterialien und Betriebsverfahren berücksichtigt werden

9.4. Vorläufige Notfallaktualisierungen müssen herausgegeben werden, wenn eine wesentliche organisatorische Änderung, eine rechtliche Vorgabe oder eine kritische Feststellung dazu führt, dass aktuelle Pläne oder diese Richtlinie nicht mehr tragfähig sind.

10. Verwandte Richtlinien und Verknüpfungen

10.1. Diese Richtlinie wird in Abstimmung mit den folgenden Schlüsseldokumenten angewendet:

10.1.1. P1 – Richtlinie zur Informationssicherheit: Legt die Anforderungen an risikobasierte, resiliente Betriebsabläufe unter allen Bedingungen fest.

10.1.2. P5 – Richtlinie zum Änderungsmanagement: Stellt sicher, dass alle wiederherstellungsbezogenen Konfigurations- oder Infrastrukturänderungen dokumentierten und genehmigten Workflows folgen.

10.1.3. P14 – Richtlinie zur Datenaufbewahrung und -vernichtung: Regelt den Lebenszyklus von Backup-Medien und wiederhergestellten Daten, die in Kontinuitätsmaßnahmen verwendet werden.

10.1.4. P15 – Richtlinie für Backup und Wiederherstellung: Verankert Kontrollen für Backup-Häufigkeit, Sicherheit und Verifizierung der Wiederherstellung.

10.1.5. P18 – Richtlinie zu kryptographischen Kontrollen: Stellt sicher, dass Wiederherstellungsprozesse Verschlüsselungs- und Vertraulichkeitsstandards einhalten.

10.1.6. P22 – Richtlinie zur Protokollierung und Überwachung: Unterstützt die Erkennung und Eskalation von Ereignissen mit Auswirkungen auf die Kontinuität.

10.1.7. P30 – Incident-Response-Richtlinie: Definiert Eindämmung, Eskalation und Ursachenanalyse im Einklang mit Kontinuitätsauslösern.

10.1.8. P33 – Richtlinie zur Audit- und Compliance-Überwachung: Validiert die Integrität und Wirksamkeit von Kontinuitäts- und Wiederherstellungspraktiken über Systeme und Prozesse hinweg.

11. Referenzstandards und Rahmenwerke

11.1. Diese Richtlinie ist an international anerkannten Standards für die Aufrechterhaltung des Geschäftsbetriebs und die Notfallwiederherstellung ausgerichtet und unterstützt Auditierbarkeit, Resilienz und Compliance.

11.2. ISO/IEC 27002

11.2.1. Anhang A, Maßnahme 5.29 – Informationssicherheit bei Störungen: Fordert die Aufrechterhaltung von Sicherheitskontrollen unter nachteiligen Bedingungen.

11.2.2. Anhang A, Maßnahme 5.30 – IKT-Bereitschaft zur Aufrechterhaltung des Geschäftsbetriebs: Verlangt die Vorbereitung, Tests und Validierung von IKT-Wiederherstellungsfähigkeiten.

11.3. ISO 22301:2019 – Business-Continuity-Managementsysteme

11.3.1. Stellt das Rahmenwerk bereit, um BCM-Praktiken im Einklang mit organisatorischen Zielen und Risikoschwellen einzuführen, umzusetzen und aufrechtzuerhalten.

11.4. NIST SP 800-34 Rev.1 – Leitfaden zur Notfallplanung

11.4.1. Beschreibt bewährte Verfahren für Notfallpläne von IT-Systemen, einschließlich der Entwicklung von Kontinuitätsstrategien, Auswirkungsanalysen und Plantests.

11.5. EU-DSGVO (2016/679)

11.5.1. Artikel 32 – Sicherheit der Verarbeitung: Verlangt die Resilienz von Verarbeitungssystemen sowie die zeitnahe Wiederherstellung der Verfügbarkeit und des Zugangs zu personenbezogenen Daten nach einem Vorfall.

11.6. EU-NIS2-Richtlinie (2022/2555)

11.6.1. Artikel 21(2)(f): Verlangt Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs und zum Krisenmanagement zur Unterstützung der Sicherheit von Netz- und Informationssystemen.

11.7. EU DORA (2022/2554)

11.7.1. Artikel 10 – IKT-Business-Continuity: Verlangt von Finanzunternehmen die Entwicklung und Erprobung von IKT-Kontinuitätsplänen, einschließlich risikobasierter RTO/RPO und Failover-Fähigkeiten.

11.8. COBIT 2019

11.8.1. DSS04 – Kontinuität managen: Umfasst alle Aspekte der Kontinuitätsplanung, einschließlich Bedrohungsidentifikation, Auswirkungsanalyse, Wiederherstellungsstrategie und regelmäßiger Tests.