| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Fügen Sie hier den Namen der eingetragenen juristischen Person ein | | | | | | | |
| Dokumentnummer:<br>P15 | | | | | Dokumenttitel:<br>**Richtlinie für Datensicherung und Wiederherstellung** | | | | | | | |
| Version:<br>1.0 | | Datum des Inkrafttretens:<br>01.01.2025 | | | Dokumentenverantwortlicher: | | | | | | | |
| X | Richtlinie | | Standard | | Verfahren | | Formular | | Register | | Sonstiges | |

| **Änderungshistorie** | | | | |
|---|---|---|---|---|
| **Änderungsnummer** | **Änderungsdatum** | **Änderungen** | **Geprüft von** | **Prozessverantwortlicher** |
| | | | | |
| | | | | |

| **Genehmigungen** | | | |
|---|---|---|---|
| **Name** | **Position** | **Datum** | **Unterschrift** |
| | | | |
| | | | |

In Übereinstimmung mit Standards und Vorschriften

| Standard/Vorschrift | Klausel/Artikel | Kommentar |
|---|---|---|
| ISO/IEC 27001:2022 | Klauseln 6.1.3, 8. | Risikobehandlung, Planung und operative Sicherungskontrollen |
| ISO/IEC 27002:2022 | Maßnahmen 8.13, 5.28, 5. | Backup-Management, sichere Entsorgung |
| NIST SP 800-53 Rev.5 | CP-9, CP-10, SI-12, MP-6 | Anforderungen an Systemsicherungen, Wiederherstellung und Medienbereinigung |
| EU-DSGVO | Artikel 32, Erwägungsgrund 49 | Wiederherstellung und Verfügbarkeit personenbezogener Daten, Aufrechterhaltung des Geschäftsbetriebs |
| EU NIS2 | Artikel 21(2)(c-e) | Backup- und Kontinuitätskontrollen zur Stärkung der Resilienz |
| EU DORA | Artikel 10, 11 | Anforderungen des Finanzsektors an Backup, Wiederherstellung und Tests |
| COBIT 2019 | DSS01, DSS04, MEA | Backup-Betrieb, Kontinuität und Überwachung der Compliance |

## 1. Zweck

1.1 Zweck dieser Richtlinie ist es, verbindliche Anforderungen für die Datensicherung und Wiederherstellung von Daten, Systemen und Anwendungen festzulegen, um Resilienz, Datenintegrität und die Aufrechterhaltung des Geschäftsbetriebs zu unterstützen.

**1.2 Die Richtlinie legt ein standardisiertes Rahmenwerk fest, um:**

1.2.1 Organisationsdaten vor Verlust infolge von Löschung, Beschädigung, Ausfällen oder Cyberangriffen zu schützen

1.2.2 Wiederherstellungsvorgaben durch klare Parameter für RTO (Recovery Time Objective) und RPO (Recovery Point Objective) zu definieren

1.2.3 Backup-Abläufe in das übergeordnete Informationssicherheitsmanagementsystem (ISMS) sowie in die Business-Continuity- und Disaster-Recovery-Pläne (BCP/DRP) zu integrieren

1.2.4 die Einhaltung anwendbarer Gesetze und branchenspezifischer Vorschriften zur Verfügbarkeit und Wiederherstellbarkeit sicherzustellen

1.3 Die Richtlinie setzt die Maßnahmen der ISO/IEC 27001:2022 in Bezug auf sichere Datenentsorgung (5.28), Resilienz (5.29) und operative Wiederherstellung (8.13) um und orientiert sich an Best Practices aus ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, DSGVO, DORA und NIS2.

## 2. Geltungsbereich

**2.1 Diese Richtlinie gilt für:**

2.1.1 alle geschäftskritischen und operativen Systeme innerhalb des ISMS-Geltungsbereichs

2.1.2 alle strukturierten und unstrukturierten Geschäftsdaten einschließlich Datenbanken, Dateien, E-Mails und Konfigurationen

2.1.3 alle Umgebungen – On-Premises, Cloud, hybrid sowie Remote- und ausgelagerte Standorte

2.1.4 sämtliches Personal, das für die Verwaltung, Durchführung, Prüfung oder Wiederherstellung von Backup-Prozessen verantwortlich ist

**2.2 Sie gilt außerdem für:**

2.2.1 Backup-Medien und -Infrastruktur, einschließlich physischer Bänder, virtueller Appliances, Festplattensnapshots und cloudbasierter Backup-Lösungen

2.2.2 Drittanbieter, die vertraglich mit dem Hosting, der Verwaltung oder der Verarbeitung von Organisations-Backups beauftragt sind

2.2.3 die Sicherung von Protokollen, Konfigurationen, Prüfpfaden und betriebsrelevanter Dokumentation zur Aufrechterhaltung des Geschäftsbetriebs

2.3 Systeme, die ausdrücklich von der Datensicherung ausgenommen sind, müssen dokumentiert, einer Risikoanalyse unterzogen und vom ISMS-Manager sowie dem Systemverantwortlichen formell genehmigt werden.

**3. Ziele**

3.1 Sicherstellen, dass alle kritischen Systeme und Daten zuverlässig mit ausreichender Frequenz, Redundanz und geeigneten Sicherheitskontrollen gesichert werden.

3.2 Wiederherstellungsmechanismen bereitstellen, die die definierten RTO- und RPO-Vorgaben im Einklang mit Business-Impact-Analysen erfüllen.

3.3 Eine vollständige Dokumentation von Backup-Verfahren, Aufbewahrungsplänen, Rollen und Technologien aufrechterhalten.

3.4 Die Wirksamkeit von Backup-Abläufen durch systematische Wiederherstellungstests, Protokollierung von Ausfällen und Nachverfolgung von Maßnahmen zur Mängelbehebung validieren.

3.5 Backup-Daten über ihren gesamten Lebenszyklus vor unbefugtem Zugriff, Veränderung oder Zerstörung schützen.

**3.6 Die Einhaltung folgender Anforderungen ermöglichen:**

3.6.1 operative und kontinuitätsbezogene Kontrollanforderungen der ISO/IEC 27001

3.6.2 NIST SP 800-53 CP- und MP-Familien für Backup und Bereinigung

3.6.3 Artikel 32 und Erwägungsgrund 49 der DSGVO zur Wiederherstellung des Zugriffs auf personenbezogene Daten

3.6.4 Artikel 10 DORA und Artikel 21 NIS2 für IKT-Kontinuität und Resilienz

3.7 Sicherstellen, dass Backup-Dienstleistungen Dritter vertragliche und regulatorische Sicherheitsverpflichtungen erfüllen, einschließlich Verschlüsselung, Entsorgung und Benachrichtigungsprotokollen.

**4. Rollen und Verantwortlichkeiten**

**4.1 Geschäftsleitung**

4.1.1 Genehmigt diese Richtlinie und stellt sicher, dass geschäftskritische Systeme durch freigegebene Backup- und Wiederherstellungsverfahren angemessen geschützt werden.

4.1.2 Trägt die Verantwortung dafür, dass Backup-Abläufe angemessen ausgestattet und regelmäßig auf regulatorische Compliance überprüft werden.

**4.2 Chief Information Security Officer (CISO)**

4.2.1 Ist Eigentümer dieser Richtlinie und stellt die Ausrichtung auf übergeordnete Rahmenwerke für Informationssicherheit, Risiko und Kontinuität sicher.

4.2.2 Überwacht die Integration von Backup-Verfahren in BCP/DRP, Incident Response und Resilienzplanung.

4.2.3 Prüft Backup-Ausnahmen und bewertet Vorschläge zur Risikoakzeptanz bei Ausschlüssen kritischer Systeme.

[ ... 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 einmal jährlich oder früher zu überprüfen, ausgelöst durch:**

9.1.1 Änderungen der Strategie zur Aufrechterhaltung des Geschäftsbetriebs oder der Disaster Recovery

9.1.2 neue regulatorische oder rechtliche Verpflichtungen, die sich auf Backup-Frequenz oder Datenaufbewahrung auswirken

9.1.3 Änderungen an Systemarchitektur, Backup-Werkzeugen oder Dienstleistern

9.1.4 wesentliche Vorfälle oder Auditfeststellungen im Zusammenhang mit Datenverlust oder Ausfällen bei der Wiederherstellung

**9.2 Die Überprüfung ist durch den CISO in Zusammenarbeit mit folgenden Stellen zu koordinieren:**

9.2.1 IT-Infrastruktur und Betrieb

9.2.2 Interne Revision und Compliance-Funktion

9.2.3 Datenschutzbeauftragter (DSB)

9.2.4 Business-Continuity- und Disaster-Recovery-Teams

**9.3 Backup-Zeitpläne, Systemeinschlusslisten, Wiederherstellungsdokumentation und Ausnahmeprotokolle sind parallel zu überprüfen, um Folgendes sicherzustellen:**

9.3.1 Genauigkeit der Backup-Abdeckung für alle kritischen Assets

9.3.2 Einhaltung der RTO-/RPO- und Aufbewahrungsanforderungen

9.3.3 Vollständigkeit der Testprotokolle und Vorfallberichte

9.3.4 Behebung zuvor identifizierter Kontrolllücken

**9.4 Alle Aktualisierungen müssen:**

9.4.1 versionskontrolliert sein und im ISMS-Dokumentenrepository aufbewahrt werden

9.4.2 eine Zusammenfassung der Änderungen und deren Begründung enthalten

9.4.3 von der Geschäftsleitung genehmigt werden

9.4.4 sämtlichem betroffenen technischen und fachlichen Personal kommuniziert werden

**10. Zugehörige Richtlinien und Verknüpfungen**

**10.1 Diese Richtlinie unterstützt unmittelbar die folgenden zugehörigen Dokumente und steht mit ihnen in Wechselwirkung:**

10.1.1 P6 - Risikomanagement-Richtlinie: Legt die risikobasierte Priorisierung des Backup-Schutzes für Systeme und Services fest.

10.1.2 P12 - Richtlinie für Asset-Management: Stellt sicher, dass für die Datensicherung geeignete Systeme inventarisiert und mit Lebenszyklusverfolgung und Klassifizierung verknüpft sind.

10.1.3 P13 - Richtlinie zur Datenklassifizierung und Kennzeichnung: Gibt vor, für welche Datenkategorien Backups erforderlich sind, einschließlich Kennzeichnungsmetadaten zur Priorisierung.

10.1.4 P14 - Richtlinie zur Datenaufbewahrung und Entsorgung: Koordiniert die Backup-Aufbewahrung mit regulatorischen Aufbewahrungsgrenzen und der ordnungsgemäßen Entsorgung abgelaufener Medien.

10.1.5 P16 - Richtlinie zur Datenmaskierung und Pseudonymisierung: Unterstützt Datenminimierung beim Backup sensibler Datenbestände.

10.1.6 P30 - Incident-Response-Richtlinie (P30): Wird bei Backup-Fehlern, Wiederherstellungsproblemen oder einer Kompromittierung von Backup-Speichern aktiviert.

10.2 Diese miteinander verknüpften Richtlinien bilden ein kohärentes Rahmenwerk, das sicherstellt, dass die Backup-Governance in das übergeordnete ISMS und die Strategie der Organisation zur operativen Resilienz eingebettet ist.

## 11. Referenzstandards und Rahmenwerke

### 11.1 ISO/IEC 27001:

11.1.1 Klausel 6.1.3 - Risikobehandlungsplan: Unterstützt die risikobasierte Priorisierung von Backups und die Planung der Wiederherstellung.

11.1.2 Klausel 8.1 - Operative Planung und Steuerung: Integriert Wiederherstellungs- und Kontinuitätskontrollen als Teil operativer Schutzmaßnahmen.

11.1.3 Anhang A Maßnahme 5.28 - Sichere Entsorgung oder Wiederverwendung von Geräten: Behandelt die sichere Bereinigung von Backup-Medien.

11.1.4 Anhang A Maßnahme 5.29 - Informationssicherheit bei Störungen: Stellt Wiederherstellungsfähigkeiten während Vorfällen oder Katastrophen sicher.

11.1.5 Anhang A Maßnahme 8.13 - Informationssicherung: Wird unmittelbar durch geplante, getestete und sichere Backup-Abläufe adressiert.

11.2 ISO/IEC 27002:2022 - Maßnahmen 8.13, 5.28, 5.: Diese Maßnahmen bekräftigen die Anforderung an regelmäßige Backups, Integritätsvalidierung und Wiederherstellungsplanung in allen IT-Umgebungen.

### 11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - System Backup: Legt umfassende Backup-Verfahren fest, einschließlich ausgelagerter Speicherung und Wiederherstellungstests.

11.3.2 CP-10 - System Recovery and Restoration: Verlangt validierte Verfahren für die vollständige oder teilweise Wiederherstellung im Einklang mit den Wiederherstellungszielen.

11.3.3 MP-6 - Media Sanitization: Stellt den sicheren Umgang mit veralteten Backup-Medien sicher.

11.3.4 SI-12 - Information Handling Procedures: Bekräftigt Backup- und Wiederherstellungsverantwortlichkeiten für sensible Daten.

### 11.4 EU-DSGVO (2016/679):

11.4.1 Artikel 32 - Sicherheit der Verarbeitung: Verlangt Wiederherstellungsfähigkeiten und Schutzmaßnahmen für die Datenverfügbarkeit, insbesondere für personenbezogene Daten.

11.4.2 Erwägungsgrund 49: Unterstützt Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs und Disaster Recovery, einschließlich sicherer Backups als Teil der organisatorischen Resilienz.

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

11.5.1 Artikel 21(2)(c-e): Verlangt technische und organisatorische Maßnahmen, einschließlich Backup- und Kontinuitätskontrollen, um die Resilienz von Diensten sicherzustellen.

### 11.6 EU DORA (2022/2554):

11.6.1 Artikel 10 - IKT-Business-Continuity: Verlangt von Finanzunternehmen vollständige Daten-Backups, Wiederherstellung und Kontinuitätsplanung.

11.6.2 Artikel 11 - Tests von IKT-Business-Continuity-Plänen: Betont die Validierung der Wiederherstellungsfähigkeit durch regelmäßige Tests.

### 11.7 COBIT 2019:

11.7.1 DSS01 - Managed Operations: Unterstützt die zuverlässige Erbringung von Services durch geschützte Datenverfügbarkeit.

11.7.2 DSS04 - Managed Continuity: Definiert strategische und operative Kontinuitätskontrollen, einschließlich validierter Backups.

11.7.3 MEA03 - Monitor, Evaluate, and Assess Compliance: Verlangt die regelmäßige Überprüfung von Kontinuitätsmaßnahmen, einschließlich der Kontrollwirksamkeit von Backup-Kontrollen.