



Author	Dipl.-Ing. Daniel Mrskos, BSc
Funktion	CEO von Security mit Passion, Penetration Tester, Mentor, FH-Lektor, NIS Prüfer
Datum	14. Juni 2024
	
Zertifizierungen	CSOM, CRTL, eCPTXv2, eWPTXv2, CCD, eCTHPv2, CRTE, CRTO, eCMAP, PNPT, eCPPTv2, eWPT, eCIR, CRTP, CARTP, PAWSP, eMAPT, eCXD, eCDFP, BTL1 (Gold), CAPEN, eEDA, OSWP, CNSP, Comptia Pentest+, ITIL Foundation V3, ICCA, CCNA, eJPTv2, Developing Security Software (LFD121), CAP, Checkmarx Security Champion
LinkedIN	<a href="https://www.linkedin.com/in/dipl-ing-daniel-mrskos-bsc-0720081ab/">https://www.linkedin.com/in/dipl-ing-daniel-mrskos-bsc-0720081ab/</a>
Website	<a href="https://security-mit-passion.at">https://security-mit-passion.at</a>

////////////////////////////////////

## Richtlinie zur Datensicherung

**Datum:** [Heutiges Datum]

### Einleitung

Diese Richtlinie zur Datensicherung definiert die Anforderungen und Maßnahmen zur Sicherstellung einer sicheren und effektiven Sicherung von Unternehmensdaten bei [Unternehmen]. Diese Richtlinie basiert auf den Standards ISO 27001:2022, ISO 27002:2022, CIS Controls v8, BSI C5:2020, der Cloud Controls Matrix (CCM), dem NIST Cybersecurity Framework, dem NIS2 Draft, der OH SzA für KRITIS, dem European Cyber Resilience Act und DORA.

### Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer, Berater, Zeitarbeitskräfte, Praktikanten und mit Dritten verbundene Personen, die für die Sicherung und Wiederherstellung von Unternehmensdaten bei [Unternehmen] verantwortlich sind.

////////////////////////////////////

## Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie zur Datensicherung mit den relevanten Sicherheitsstandards und -richtlinien zu gewährleisten. Sie zeigt die Zuordnung der einzelnen Policy-Komponenten zu den spezifischen Anforderungen der Standards wie ISO 27001:2022, CIS Controls V8, BSI C5:2020, der Cloud Controls Matrix (CCM), dem NIST Cybersecurity Framework, dem NIS2 Draft, der OH SzA für KRITIS, dem European Cyber Resilience Act und DORA. Dies erleichtert die Nachverfolgung und Überprüfung, dass alle notwendigen Sicherheitsmaßnahmen implementiert sind und ermöglicht eine klare, transparente Dokumentation unserer Compliance-Verpflichtungen.

Policy-Komponente	ISO 27001:2022 / 27002:2022	TISAX	CIS Controls V8	BSI C5:2020	CCM	NIST CSF	NIS2	OH SzA	European CRA	DORA
Backup-Strategie	8.11.1, 8.11.2	1.1.1, 1.2.1	11.1, 11.2	ORP1, ORP2	DSI-01, DSI-02	PR.IP-1, PR.IP-2	Artikel 5, 6.1	Abschnitt 2.3	Artikel 23	Artikel 4
Backup-Frequenz und -Zeitplan	8.11.3, 8.11.4	2.1.1, 2.1.2	12.1, 12.2	ORP3, ORP4	DSI-03, DSI-04	PR.IP-3, PR.IP-4	Artikel 5, 6.2	Abschnitt 2.4	Artikel 23	Artikel 4
Backup-Speicherung und -Sicherung	8.11.5, 8.11.6	3.1.1, 3.1.2	13.1, 13.2	OPS1, OPS2	DSI-05, DSI-06	PR.DS-1, PR.DS-2	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Wiederherstellung und Testen der Backups	8.11.7, 8.11.8	3.2.1, 3.2.2	14.1, 14.2	OPS3, OPS4	DSI-07, DSI-08	PR.DS-3, PR.DS-4	Artikel 6.4	Abschnitt 2.6	Artikel 23	Artikel 4
Zugriffskontrollen für Backup-Daten	9.1.2, 9.1.3	4.1.1, 4.1.2	15.1, 15.2	OPS5, OPS6	IAM-01, IAM-02	PR.AC-1, PR.AC-2	Artikel 6.5	Abschnitt 2.7	Artikel 23	Artikel 4
Überwachung und Überprüfung der Backup-Prozesse	9.4.1, 9.4.2	4.2.1, 4.2.2	16.1, 16.2	ORP5, ORP6	IVS-01, IVS-02	DE.CM-1, DE.CM-2	Artikel 6.6	Abschnitt 2.8	Artikel 23	Artikel 4

## Richtlinien und Anforderungen

### Backup-Strategie

Eine umfassende Backup-Strategie muss entwickelt und implementiert werden (ISO 27001: 8.11.1, 8.11.2). Diese Strategie muss die Anforderungen an die Datensicherung und die Verantwortlichkeiten der beteiligten Personen klar definieren (CIS Controls 11.1, 11.2, TISAX 1.1.1, 1.2.1). Die Strategie muss regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie den aktuellen Sicherheitsanforderungen entspricht (BSI C5: ORP1, ORP2, CCM DSI-01, DSI-02).

### Backup-Frequenz und -Zeitplan

Die Frequenz und der Zeitplan für die Erstellung von Backups müssen festgelegt und eingehalten werden (ISO 27001: 8.11.3, 8.11.4). Diese müssen den Anforderungen des Unternehmens entsprechen und sicherstellen, dass Daten regelmäßig gesichert werden (CIS Controls 12.1, 12.2, TISAX 2.1.1, 2.1.2). Regelmäßige Überprüfungen sind notwendig, um die Einhaltung des Zeitplans sicherzustellen (BSI C5: ORP3, ORP4, CCM DSI-03, DSI-04).

### Backup-Speicherung und -Sicherung

Gesicherte Daten müssen an sicheren Orten gespeichert werden (ISO 27001: 8.11.5, 8.11.6). Dies beinhaltet die Nutzung von physischen und Cloud-Speichern, die vor unbefugtem Zugriff und physischen Schäden geschützt sind (CIS Controls 13.1, 13.2, TISAX 3.1.1, 3.1.2). Es müssen regelmäßige Sicherheitsüberprüfungen der Speicherorte durchgeführt werden (NIST CSF PR.DS-1, PR.DS-2, BSI C5: OPS1, OPS2, CCM DSI-05, DSI-06).

### Wiederherstellung und Testen der Backups

Die Wiederherstellungsprozesse müssen regelmäßig getestet werden, um sicherzustellen, dass Daten im Falle eines Vorfalls schnell und vollständig wiederhergestellt werden können (ISO 27001: 8.11.7, 8.11.8). Dies beinhaltet die Durchführung regelmäßiger Wiederherstellungstests und die Dokumentation der Ergebnisse (CIS Controls 14.1, 14.2, TISAX 3.2.1, 3.2.2). Alle Tests müssen überprüft und analysiert werden, um Verbesserungspotenziale zu identifizieren (NIST CSF PR.DS-3, PR.DS-4, BSI C5: OPS3, OPS4, CCM DSI-07, DSI-08).

**Zugriffskontrollen für Backup-Daten**

Der Zugriff auf Backup-Daten muss streng kontrolliert werden (ISO 27001: 9.1.2, 9.1.3). Dies umfasst die Implementierung von Zugriffskontrollen und Authentifizierungsmechanismen, um unbefugten Zugriff zu verhindern (CIS Controls 15.1, 15.2, TISAX 4.1.1, 4.1.2). Regelmäßige Überprüfungen der Zugriffskontrollen sind notwendig, um die Sicherheit der Daten zu gewährleisten (NIST CSF PR.AC-1, PR.AC-2, BSI C5: OPS5, OPS6, CCM IAM-01, IAM-02).

**Überwachung und Überprüfung der Backup-Prozesse**

Alle Backup-Prozesse müssen kontinuierlich überwacht und regelmäßig überprüft werden (ISO 27001: 9.4.1, 9.4.2). Die Überwachung muss sicherstellen, dass alle Backups erfolgreich durchgeführt werden und keine Daten verloren gehen (CIS Controls 16.1, 16.2, TISAX 4.2.1, 4.2.2). Die Ergebnisse der Überwachung müssen dokumentiert und analysiert werden, um Verbesserungspotenziale zu identifizieren (NIST CSF DE.CM-1, DE.CM-2, BSI C5: ORP5, ORP6, CCM IVS-01, IVS-02).

**Verantwortliche**

Die Implementierung und Einhaltung dieser Richtlinie liegt in der Verantwortung des IT-Sicherheitsbeauftragten und des Backup Management Teams. Alle Mitarbeiter sind verpflichtet, sich an diese Richtlinie zu halten und jegliche Verstöße umgehend zu melden.

**Quellen und Referenzen**

Quelle	Zweck	Link
ISO27001:2022	Aufbau und Implementierung eines ISMS	<a href="#">ISO 27001:2022</a>
CIS Controls v8	Sicherheitsmaßnahmen gegen Cyberangriffe	<a href="#">CIS Controls v8</a>
BSI C5:2020	Cloud Security Standard	<a href="#">BSI C5:2020</a>
Cloud Controls Matrix (CCM)	Sicherheitskontrollen für Cloud-Dienste	<a href="#">Cloud Controls Matrix</a>
NIST Cybersecurity Framework	Rahmenwerk zur Verbesserung der Cybersicherheit	<a href="#">NIST CSF</a>
NIS2 Draft	EU-Richtlinie zur Netz- und Informationssicherheit	<a href="#">NIS2 Draft</a>
OH SzA für KRITIS	Orientierungshilfe Angriffserkennung für Kritische Infrastrukturen	<a href="#">OH SzA</a>
European Cyber Resilience Act	EU-Verordnung zur Cyber-Resilienz	<a href="#">European CRA</a>
Digital Operational Resilience Act (DORA)	EU-Verordnung zur digitalen operationellen Resilienz	<a href="#">DORA</a>

Diese Quellen und Referenzen bieten umfassende Leitlinien und Best Practices für die Entwicklung und Implementierung von Sicherheitsmaßnahmen sowie für die Einhaltung der relevanten Standards und Richtlinien. Sie dienen als Grundlage und Unterstützung bei der Implementierung und Aufrechterhaltung eines sicheren Backup-Managements bei [Unternehmen].

**Dokumentinformationen**

**Titel:** Richtlinie zur Datensicherung  
**Version:** 1.0  
**Datum:** [Heutiges Datum]  
**Verantwortlich:** IT-Sicherheitsbeauftragter  
**Genehmigt von:** [Name der genehmigenden Person]

**Nächste Überprüfung:** [Datum der nächsten Überprüfung]