


|   |   |
|---|---|
| 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, eCDFF, 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 Nutzung von Cloud-Diensten

**Datum:** [Heutiges Datum]

### Einleitung

Diese Richtlinie zur Nutzung von Cloud-Diensten definiert die Anforderungen und Maßnahmen zur Sicherstellung einer sicheren und verantwortungsvollen Nutzung von Cloud-Computing-Services 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 Cloud-Computing-Services für [Unternehmen] nutzen oder verwalten.

## Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie zur Nutzung von Cloud-Diensten 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<br>27001:2022<br>/<br>27002:2022 | TISAX           | CIS<br>Controls<br>V8 | BSI<br>C5:2020 | CCM               | NIST<br>CSF         | NIS2              | OH SzA           | European<br>CRA | DORA         |
|---|--------------------------------------|-----------------|-----------------------|----------------|-------------------|---------------------|-------------------|------------------|-----------------|--------------|
| Auswahl von Cloud-Dienstleistern        | 5.22, 6.1.1                          | 1.1.1,<br>1.2.1 | 1.1, 1.2              | ORP1,<br>ORP2  | AIS-01,<br>AIS-02 | ID.RA-1,<br>ID.RA-2 | Artikel<br>5, 6.1 | Abschnitt<br>2.3 | Artikel 23      | Artikel<br>4 |
| Vertragsmanagement mit Cloud-Anbietern  | 7.1.2, 7.1.3                         | 2.1.1,<br>2.1.2 | 2.1, 2.2              | ORP3,<br>ORP4  | AIS-03            | ID.RA-3,<br>ID.RA-4 | Artikel<br>5, 6.2 | Abschnitt<br>2.4 | Artikel 23      | Artikel<br>4 |
| Datensicherheit und Datenschutz         | 8.2.3, 8.2.4                         | 3.1.1,<br>3.1.2 | 3.1, 3.2              | OPS1,<br>OPS2  | DSI-01,<br>DSI-02 | PR.DS-1,<br>PR.DS-2 | Artikel<br>6.3    | Abschnitt<br>2.5 | Artikel 23      | Artikel<br>4 |
| Zugriffskontrolle und Authentifizierung | 9.1.2, 9.1.3                         | 3.2.1,<br>3.2.2 | 4.1, 4.2              | OPS3,<br>OPS4  | IAM-01,<br>IAM-02 | PR.AC-1,<br>PR.AC-2 | Artikel<br>6.4    | Abschnitt<br>2.6 | Artikel 23      | Artikel<br>4 |
| Monitoring und Incident Response        | 9.4.1, 9.4.2                         | 4.1.1,<br>4.1.2 | 5.1, 5.2              | OPS5,<br>OPS6  | IVS-01,<br>IVS-02 | DE.CM-1,<br>DE.CM-2 | Artikel<br>6.5    | Abschnitt<br>2.7 | Artikel 23      | Artikel<br>4 |
| Schulung und Sensibilisierung           | 6.3.1, 6.3.2                         | 4.2.1,<br>4.2.2 | 6.1, 6.2              | ORP5,<br>ORP6  | STA-01,<br>STA-02 | PR.AT-1,<br>PR.AT-2 | Artikel<br>6.6    | Abschnitt<br>2.8 | Artikel 23      | Artikel<br>4 |

## Richtlinien und Anforderungen

### Auswahl von Cloud-Dienstleistern

Die Auswahl von Cloud-Dienstleistern muss sorgfältig und auf Basis klar definierter Kriterien erfolgen (ISO 27001: 5.22, 6.1.1). Dies beinhaltet die Bewertung der Sicherheitsmaßnahmen und der Einhaltung von Datenschutzvorschriften durch den Dienstleister (CIS Controls 1.1, 1.2, TISAX 1.1.1, 1.2.1). Eine Risikoanalyse ist durchzuführen, um potenzielle Schwachstellen zu identifizieren und zu bewerten (BSI C5: ORP1, ORP2, CCM AIS-01, AIS-02).

### Vertragsmanagement mit Cloud-Anbietern

Verträge mit Cloud-Dienstleistern müssen klare Regelungen zur Datensicherheit und zum Datenschutz enthalten (ISO 27001: 7.1.2, 7.1.3). Dies umfasst Vertraulichkeitsvereinbarungen, Sicherheitsanforderungen und Regelungen zur Incident Response (CIS Controls 2.1, 2.2, TISAX 2.1.1, 2.1.2). Verträge müssen regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie den aktuellen Sicherheitsanforderungen entsprechen (BSI C5: ORP3, ORP4, CCM AIS-03).

### Datensicherheit und Datenschutz

Der Schutz von Daten in der Cloud muss jederzeit gewährleistet sein (ISO 27001: 8.2.3, 8.2.4). Dies beinhaltet die Verschlüsselung von Daten, sowohl bei der Übertragung als auch bei der Speicherung, und die Implementierung von Maßnahmen zur Datensicherung (CIS Controls 3.1, 3.2, TISAX 3.1.1, 3.1.2). Es müssen regelmäßige Überprüfungen und Audits durchgeführt werden, um die Einhaltung der Sicherheitsrichtlinien sicherzustellen (NIST CSF PR.DS-1, PR.DS-2, BSI C5: OPS1, OPS2, CCM DSI-01, DSI-02).

### Zugriffskontrolle und Authentifizierung

Der Zugang zu Cloud-Diensten muss strikt kontrolliert und gesichert werden (ISO 27001: 9.1.2, 9.1.3). Dies beinhaltet die Implementierung von Multi-Faktor-Authentifizierung und strikten Zugriffskontrollen, um unbefugten Zugriff zu verhindern (CIS Controls 4.1, 4.2, TISAX 3.2.1,

3.2.2). Regelmäßige Überprüfungen und Aktualisierungen der Zugriffskontrollen sind notwendig, um die Sicherheit zu gewährleisten (NIST CSF PR.AC-1, PR.AC-2, BSI C5: OPS3, OPS4, CCM IAM-01, IAM-02).

Monitoring und Incident Response

Alle Aktivitäten in der Cloud müssen kontinuierlich überwacht und protokolliert werden (ISO 27001: 9.4.1, 9.4.2). Dies umfasst die Einrichtung von Monitoring-Systemen, die in der Lage sind, ungewöhnliche Aktivitäten zu erkennen und zu melden (CIS Controls 5.1, 5.2, TISAX 4.1.1, 4.1.2). Ein effektives Incident Response Management muss implementiert werden, um auf Sicherheitsvorfälle schnell und angemessen reagieren zu können (NIST CSF DE.CM-1, DE.CM-2, BSI C5: OPS5, OPS6, CCM IVS-01, IVS-02).

Schulung und Sensibilisierung

Alle Mitarbeiter müssen regelmäßig Schulungen zur sicheren Nutzung von Cloud-Diensten durchlaufen (ISO 27001: 6.3.1, 6.3.2). Diese Schulungen müssen die aktuellen Bedrohungen, Sicherheitsmaßnahmen und Best Practices abdecken (CIS Controls 6.1, 6.2, TISAX 4.2.1, 4.2.2). Sensibilisierungsmaßnahmen müssen implementiert werden, um sicherzustellen, dass alle Mitarbeiter über die aktuellen Sicherheitsanforderungen informiert sind (NIST CSF PR.AT-1, PR.AT-2, BSI C5: ORP5, ORP6, CCM STA-01, STA-02).

Verantwortliche

Die Implementierung und Einhaltung dieser Richtlinie liegt in der Verantwortung des IT-Sicherheitsbeauftragten und des Cloud 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 einer sicheren Nutzung von Cloud-Diensten bei [Unternehmen].

Dokumentinformationen

**Titel:** Richtlinie zur Nutzung von Cloud-Diensten  
**Version:** 1.0  
**Datum:** [Heutiges Datum]  
**Verantwortlich:** IT-Sicherheitsbeauftragter  
**Genehmigt von:** [Name der genehmigenden Person]  
**Nächste Überprüfung:** [Datum der nächsten Überprüfung]