



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	https://www.linkedin.com/in/dipl-ing-daniel-mrskos-bsc-0720081ab/
Website	https://security-mit-passion.at

Richtlinie zur Handhabung von Wechseldatenträgern

Datum: [Heutiges Datum]

Einleitung

Diese Richtlinie zur Handhabung von Wechseldatenträgern definiert die Anforderungen und Maßnahmen zur sicheren Nutzung, Verwaltung und Entsorgung von Wechseldatenträgern 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 Wechseldatenträger für [Unternehmen] nutzen oder verwalten.

Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie zur Handhabung von Wechseldatenträgern 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
Zulässige Nutzung von Wechseldatenträgern	8.3.1, 8.3.2	1.1.1, 1.2.1	10.1, 10.2	ORP1, ORP2	DSI-01, DSI-02	PR.AC-1, PR.AC-2	Artikel 5, 6.1	Abschnitt 2.3	Artikel 23	Artikel 4
Verschlüsselung und Schutz von Daten	8.15.1, 8.15.2	2.1.1, 2.1.2	13.1, 13.2	ORP3, ORP4	DSI-03, DSI-04	PR.DS-1, PR.DS-2	Artikel 5, 6.2	Abschnitt 2.4	Artikel 23	Artikel 4
Zugangskontrollen und Authentifizierung	9.1.2, 9.1.3	3.1.1, 3.1.2	14.1, 14.2	OPS1, OPS2	IAM-01, IAM-02	PR.AC-3, PR.AC-4	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Protokollierung und Überwachung	9.4.1, 9.4.2	3.2.1, 3.2.2	15.1, 15.2	OPS3, OPS4	IVS-01, IVS-02	DE.CM-1, DE.CM-2	Artikel 6.4	Abschnitt 2.6	Artikel 23	Artikel 4
Sichere Entsorgung von Wechseldatenträgern	8.3.3, 8.3.4	4.1.1, 4.1.2	16.1, 16.2	ORP5, ORP6	DSI-05, DSI-06	PR.DS-3, PR.DS-4	Artikel 6.5	Abschnitt 2.7	Artikel 23	Artikel 4
Schulung und Sensibilisierung	6.3.1, 6.3.2	4.2.1, 4.2.2	17.1, 17.2	ORP7, ORP8	STA-01, STA-02	PR.AT-1, PR.AT-2	Artikel 6.6	Abschnitt 2.8	Artikel 23	Artikel 4

Richtlinien und Anforderungen

Zulässige Nutzung von Wechseldatenträgern

Die Nutzung von Wechseldatenträgern muss klar geregelt und nur für autorisierte Zwecke gestattet sein (ISO 27001: 8.3.1, 8.3.2). Dies umfasst die Festlegung von Richtlinien zur erlaubten Verwendung und zur sicheren Handhabung von Wechseldatenträgern (CIS Controls 10.1, 10.2, TISAX 1.1.1, 1.2.1). Regelmäßige Überprüfungen und Aktualisierungen dieser Richtlinien sind notwendig, um die Sicherheit zu gewährleisten (BSI C5: ORP1, ORP2, CCM DSI-01, DSI-02).

Verschlüsselung und Schutz von Daten

Alle auf Wechseldatenträgern gespeicherten Daten müssen durch geeignete Verschlüsselungsmethoden geschützt werden (ISO 27001: 8.15.1, 8.15.2). Dies umfasst die Implementierung von Verschlüsselungstechnologien, um die Vertraulichkeit und Integrität der Daten zu gewährleisten (CIS Controls 13.1, 13.2, TISAX 2.1.1, 2.1.2). Regelmäßige Überprüfungen der Verschlüsselungsprotokolle sind notwendig, um die Sicherheit zu gewährleisten (NIST CSF PR.DS-1, PR.DS-2, BSI C5: ORP3, ORP4, CCM DSI-03, DSI-04).

Zugangskontrollen und Authentifizierung

Der Zugang zu Wechseldatenträgern muss strikt kontrolliert und gesichert werden (ISO 27001: 9.1.2, 9.1.3). Dies umfasst die Implementierung von Zugriffskontrollen und Authentifizierungsmechanismen, um unbefugten Zugriff zu verhindern (CIS Controls 14.1, 14.2, TISAX 3.1.1, 3.1.2). Regelmäßige Überprüfungen der Zugangskontrollen sind notwendig, um die Sicherheit der Daten zu gewährleisten (NIST CSF PR.AC-3, PR.AC-4, BSI C5: OPS1, OPS2, CCM IAM-01, IAM-02).

Protokollierung und Überwachung

Alle Aktivitäten im Zusammenhang mit der Nutzung von Wechseldatenträgern müssen kontinuierlich überwacht und protokolliert werden

(ISO 27001: 9.4.1, 9.4.2). Dies umfasst die Implementierung von Monitoring-Systemen und Protokollierungsmechanismen, um ungewöhnliche Aktivitäten zu erkennen und zu melden (CIS Controls 15.1, 15.2, TISAX 3.2.1, 3.2.2). Die Protokollierung muss regelmäßig überprüft und analysiert werden, um Sicherheitsvorfälle frühzeitig zu erkennen (NIST CSF DE.CM-1, DE.CM-2, BSI C5: OPS3, OPS4, CCM IVS-01, IVS-02).

Sichere Entsorgung von Wechseldatenträgern

Wechseldatenträger müssen sicher entsorgt werden, wenn sie nicht mehr benötigt werden (ISO 27001: 8.3.3, 8.3.4). Dies umfasst die Nutzung von Datenvernichtungsverfahren, um sicherzustellen, dass keine vertraulichen Informationen wiederhergestellt werden können (CIS Controls 16.1, 16.2, TISAX 4.1.1, 4.1.2). Alle Entsorgungsmaßnahmen müssen dokumentiert und überwacht werden, um die Einhaltung der Richtlinien sicherzustellen (NIST CSF PR.DS-3, PR.DS-4, BSI C5: ORP5, ORP6, CCM DSI-05, DSI-06).

Schulung und Sensibilisierung

Alle Mitarbeiter müssen regelmäßig Schulungen zur sicheren Handhabung von Wechseldatenträgern durchlaufen (ISO 27001: 6.3.1, 6.3.2). Diese Schulungen müssen die aktuellen Bedrohungen, Sicherheitsmaßnahmen und Best Practices abdecken (CIS Controls 17.1, 17.2, 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: ORP7, ORP8, CCM STA-01, STA-02).

Verantwortliche

Die Implementierung und Einhaltung dieser Richtlinie liegt in der Verantwortung des IT-Sicherheitsbeauftragten und des Datensicherheits-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	ISO 27001:2022
CIS Controls v8	Sicherheitsmaßnahmen gegen Cyberangriffe	CIS Controls v8
BSI C5:2020	Cloud Security Standard	BSI C5:2020
Cloud Controls Matrix (CCM)	Sicherheitskontrollen für Cloud-Dienste	Cloud Controls Matrix
NIST Cybersecurity Framework	Rahmenwerk zur Verbesserung der Cybersicherheit	NIST CSF
NIS2 Draft	EU-Richtlinie zur Netz- und Informationssicherheit	NIS2 Draft
OH SzA für KRITIS	Orientierungshilfe Angriffserkennung für Kritische Infrastrukturen	OH SzA
European Cyber Resilience Act	EU-Verordnung zur Cyber-Resilienz	European CRA
Digital Operational Resilience Act (DORA)	EU-Verordnung zur digitalen operationellen Resilienz	DORA

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 Handhabung von Wechseldatenträgern bei [Unternehmen].

Dokumentinformationen

Titel: Richtlinie zur Handhabung von Wechseldatenträgern
Version: 1.0
Datum: [Heutiges Datum]
Verantwortlich: IT-Sicherheitsbeauftragter
Genehmigt von: [Name der genehmigenden Person]
Nächste Überprüfung: [Datum der nächsten Überprüfung]

