



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

Richtlinie zum Management von Drittanbietern

Datum: [Heutiges Datum]

Einleitung

Diese Richtlinie zum Management von Drittanbietern definiert die Anforderungen und Maßnahmen zur Sicherstellung der Sicherheit und des Datenschutzes bei der Zusammenarbeit mit Drittanbietern 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 in irgendeiner Form mit Drittanbietern für [Unternehmen] zusammenarbeiten.

Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie zum Management von Drittanbietern 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
Auswahl und Bewertung von Drittanbietern	5.19, 5.20	1.1.1, 1.2.1	15.1, 15.2	ORP1, ORP2	SEF-01, SEF-02	ID.RA-1, ID.RA-2	Artikel 5, 6.1	Abschnitt 2.3	Artikel 23	Artikel 4
Vertragsmanagement	5.21, 5.22	2.1.1, 2.1.2	16.1, 16.2	ORP3, ORP4	SEF-03, SEF-04	ID.RM-1, ID.RM-2	Artikel 5, 6.2	Abschnitt 2.4	Artikel 23	Artikel 4
Sicherheitsanforderungen für Drittanbieter	5.23, 5.24	3.1.1, 3.1.2	17.1, 17.2	OPS1, OPS2	SEF-05, SEF-06	PR.IP-1, PR.IP-2	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Überwachung und Überprüfung von Drittanbietern	5.25, 5.26	4.1.1, 4.1.2	18.1, 18.2	OPS3, OPS4	SEF-07, SEF-08	DE.CM-1, DE.CM-2	Artikel 6.4	Abschnitt 2.6	Artikel 23	Artikel 4
Zugriffskontrollen und Authentifizierung	9.1.2, 9.1.3	4.2.1, 4.2.2	5.1, 5.2	OPS5, OPS6	IAM-01, IAM-02	PR.AC-1, PR.AC-2	Artikel 6.5	Abschnitt 2.7	Artikel 23	Artikel 4
Schulung und Sensibilisierung	6.3.1, 6.3.2	4.3.1, 4.3.2	19.1, 19.2	ORP5, ORP6	STA-01, STA-02	PR.AT-1, PR.AT-2	Artikel 6.6	Abschnitt 2.8	Artikel 23	Artikel 4

Richtlinien und Anforderungen

Auswahl und Bewertung von Drittanbietern

Alle Drittanbieter müssen vor ihrer Beauftragung sorgfältig ausgewählt und bewertet werden (ISO 27001: 5.19, 5.20). Dies umfasst die Überprüfung der Sicherheitsmaßnahmen und der Einhaltung von Datenschutzvorschriften durch den Drittanbieter (CIS Controls 15.1, 15.2, TISAX 1.1.1, 1.2.1). Eine Risikoanalyse ist durchzuführen, um potenzielle Schwachstellen zu identifizieren und zu bewerten (BSI C5: ORP1, ORP2, CCM SEF-01, SEF-02).

Vertragsmanagement

Verträge mit Drittanbietern müssen klare Regelungen zur Datensicherheit und zum Datenschutz enthalten (ISO 27001: 5.21, 5.22). Dies umfasst Vertraulichkeitsvereinbarungen, Sicherheitsanforderungen und Regelungen zur Incident Response (CIS Controls 16.1, 16.2, 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 SEF-03, SEF-04).

Sicherheitsanforderungen für Drittanbieter

Alle Drittanbieter müssen die Sicherheitsanforderungen von [Unternehmen] einhalten (ISO 27001: 5.23, 5.24). Dies umfasst die Implementierung von Sicherheitsmaßnahmen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten (CIS Controls 17.1, 17.2, TISAX 3.1.1, 3.1.2). Regelmäßige Audits und Überprüfungen sind notwendig, um die Einhaltung der Sicherheitsanforderungen sicherzustellen (NIST CSF PR.IP-1, PR.IP-2, BSI C5: OPS1, OPS2, CCM SEF-05, SEF-06).

Überwachung und Überprüfung von Drittanbietern

Alle Aktivitäten von Drittanbietern müssen kontinuierlich überwacht und regelmäßig überprüft werden (ISO 27001: 5.25, 5.26). Die Überwachung muss sicherstellen, dass alle Sicherheitsanforderungen eingehalten werden und keine Sicherheitsvorfälle auftreten (CIS Controls 18.1, 18.2, TISAX 4.1.1, 4.1.2). Die Ergebnisse der Überwachung müssen dokumentiert und analysiert werden, um

Verbesserungspotenziale zu identifizieren (NIST CSF DE.CM-1, DE.CM-2, BSI C5: OPS3, OPS4, CCM SEF-07, SEF-08).

Zugriffskontrollen und Authentifizierung

Der Zugang zu den Systemen und Daten von [Unternehmen] durch Drittanbieter muss strikt kontrolliert und gesichert werden (ISO 27001: 9.1.2, 9.1.3). Dies umfasst die Implementierung von Multi-Faktor-Authentifizierung und strikten Zugriffskontrollen, um unbefugten Zugriff zu verhindern (CIS Controls 5.1, 5.2, TISAX 4.2.1, 4.2.2). Regelmäßige Überprüfungen und Aktualisierungen der Zugriffskontrollen sind notwendig, um die Sicherheit zu gewährleisten (NIST CSF PR.AC-1, PR.AC-2, BSI C5: OPS5, OPS6, CCM IAM-01, IAM-02).

Schulung und Sensibilisierung

Alle Mitarbeiter und Drittanbieter müssen regelmäßig Schulungen zur Informationssicherheit durchlaufen (ISO 27001: 6.3.1, 6.3.2). Diese Schulungen müssen die aktuellen Bedrohungen, Sicherheitsmaßnahmen und Best Practices abdecken (CIS Controls 19.1, 19.2, TISAX 4.3.1, 4.3.2). Sensibilisierungsmaßnahmen müssen implementiert werden, um sicherzustellen, dass alle Beteiligten 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 Third-Party Management Teams. Alle Mitarbeiter und Drittanbieter 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 Zusammenarbeit mit Drittanbietern bei [Unternehmen].

Dokumentinformationen

Titel: Richtlinie zum Management von Drittanbietern
Version: 1.0
Datum: [Heutiges Datum]
Verantwortlich: IT-Sicherheitsbeauftragter
Genehmigt von: [Name der genehmigenden Person]
Nächste Überprüfung: [Datum der nächsten Überprüfung]