



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, CRT0, 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 zur Personalsicherheit

Datum: [Heutiges Datum]

Einleitung

Diese Richtlinie zur Personalsicherheit definiert die Anforderungen und Maßnahmen zur Sicherstellung der Sicherheit von Personalressourcen und zur Minimierung von Risiken, die durch Mitarbeiter bei [Unternehmen] entstehen können. 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 [Unternehmen] tätig sind.

Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie zur Personalsicherheit 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
Überprüfung von Mitarbeitern vor Einstellung	7.1.1, 7.1.2	1.1.1, 1.2.1	14.1, 14.2	ORP1, ORP2	GOV-01, GOV-02	ID.GV-1, ID.GV-2	Artikel 5, 6.1	Abschnitt 2.3	Artikel 23	Artikel 4
Sicherheitsrichtlinien für Mitarbeiter	7.2.1, 7.2.2	2.1.1, 2.1.2	16.1, 16.2	ORP3, ORP4	GOV-03, GOV-04	PR.IP-1, PR.IP-2	Artikel 5, 6.2	Abschnitt 2.4	Artikel 23	Artikel 4
Schulung und Sensibilisierung	6.3.1, 6.3.2	3.1.1, 3.1.2	17.1, 17.2	ORP5, ORP6	STA-01, STA-02	PR.AT-1, PR.AT-2	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Zugangskontrollen und Authentifizierung	9.1.2, 9.1.3	4.1.1, 4.1.2	5.1, 5.2	OPS1, OPS2	IAM-01, IAM-02	PR.AC-1, PR.AC-2	Artikel 6.4	Abschnitt 2.6	Artikel 23	Artikel 4
Überwachung und Meldung von Vorfällen	9.4.1, 9.4.2	4.2.1, 4.2.2	16.1, 16.2	OPS3, OPS4	IVS-01, IVS-02	DE.CM-1, DE.CM-2	Artikel 6.5	Abschnitt 2.7	Artikel 23	Artikel 4
Maßnahmen bei Austritt eines Mitarbeiters	9.5.1, 9.5.2	4.3.1, 4.3.2	17.1, 17.2	ORP7, ORP8	IVS-03, IVS-04	RS.CO-1, RS.CO-2	Artikel 6.6	Abschnitt 2.8	Artikel 23	Artikel 4

Richtlinien und Anforderungen

Überprüfung von Mitarbeitern vor Einstellung

Alle potenziellen Mitarbeiter müssen vor ihrer Einstellung gründlich überprüft werden (ISO 27001: 7.1.1, 7.1.2). Dies umfasst Hintergrundüberprüfungen und die Verifizierung der angegebenen Qualifikationen und Erfahrungen (CIS Controls 14.1, 14.2, TISAX 1.1.1, 1.2.1). Diese Maßnahmen sollen sicherstellen, dass nur vertrauenswürdige Personen Zugang zu sensiblen Informationen und Systemen erhalten (BSI C5: ORP1, ORP2, CCM GOV-01, GOV-02).

Sicherheitsrichtlinien für Mitarbeiter

Alle Mitarbeiter müssen die Sicherheitsrichtlinien und -verfahren des Unternehmens verstehen und einhalten (ISO 27001: 7.2.1, 7.2.2). Dies umfasst das Lesen und Akzeptieren der Sicherheitsrichtlinien sowie das Einhalten der festgelegten Verhaltensregeln (CIS Controls 16.1, 16.2, TISAX 2.1.1, 2.1.2). Regelmäßige Schulungen und Updates der Sicherheitsrichtlinien sind notwendig, um sicherzustellen, dass alle Mitarbeiter über die aktuellen Anforderungen informiert sind (BSI C5: ORP3, ORP4, CCM GOV-03, GOV-04).

Schulung und Sensibilisierung

Alle Mitarbeiter müssen regelmäßig Schulungen zur Informationssicherheit und Sensibilisierungsmaßnahmen 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 3.1.1, 3.1.2). 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).

Zugangskontrollen und Authentifizierung

Der Zugang zu Informationssystemen und Daten muss strikt kontrolliert und gesichert werden (ISO 27001: 9.1.2, 9.1.3). Dies umfasst die

Implementierung von Multi-Faktor-Authentifizierung und strikten Zugangskontrollen, um unbefugten Zugang zu verhindern (CIS Controls 5.1, 5.2, TISAX 4.1.1, 4.1.2). Regelmäßige Überprüfungen und Aktualisierungen der Zugangskontrollen sind notwendig, um die Sicherheit zu gewährleisten (NIST CSF PR.AC-1, PR.AC-2, BSI C5: OPS1, OPS2, CCM IAM-01, IAM-02).

Überwachung und Meldung von Vorfällen

Alle sicherheitsrelevanten Aktivitäten und Vorfälle müssen kontinuierlich überwacht und gemeldet werden (ISO 27001: 9.4.1, 9.4.2). Dies umfasst die Einrichtung von Überwachungs- und Meldesystemen, um ungewöhnliche Aktivitäten frühzeitig zu erkennen (CIS Controls 16.1, 16.2, TISAX 4.2.1, 4.2.2). Die Ergebnisse der Überwachung müssen regelmäßig überprüft und analysiert werden, um Sicherheitsvorfälle frühzeitig zu erkennen und zu beheben (NIST CSF DE.CM-1, DE.CM-2, BSI C5: OPS3, OPS4, CCM IVS-01, IVS-02).

Maßnahmen bei Austritt eines Mitarbeiters

Bei Austritt eines Mitarbeiters müssen geeignete Maßnahmen ergriffen werden, um sicherzustellen, dass der Zugang zu Informationen und Systemen ordnungsgemäß beendet wird (ISO 27001: 9.5.1, 9.5.2). Dies umfasst die Deaktivierung von Benutzerkonten, die Rückgabe von Unternehmensressourcen und die Aktualisierung von Zugangskontrolllisten (CIS Controls 17.1, 17.2, TISAX 4.3.1, 4.3.2). Regelmäßige Überprüfungen dieser Maßnahmen sind notwendig, um sicherzustellen, dass keine unbefugten Zugriffe erfolgen (NIST CSF RS.CO-1, RS.CO-2, BSI C5: ORP7, ORP8, CCM IVS-03, IVS-04).

Verantwortliche

Die Implementierung und Einhaltung dieser Richtlinie liegt in der Verantwortung des IT-Sicherheitsbeauftragten und des Human Resources 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 Personalsicherheitsstrategie bei [Unternehmen].

Dokumentinformationen

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

