



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 akzeptablen Nutzung von KI-Systemen

**Datum:** [Heutiges Datum]

### Einleitung

Diese Richtlinie zur akzeptablen Nutzung von KI-Systemen definiert die Anforderungen und Maßnahmen zur Sicherstellung einer sicheren und verantwortungsvollen Nutzung der Künstlichen Intelligenz (KI) 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 Zugang zu den KI-Ressourcen von [Unternehmen] haben.

=====

## Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie zur akzeptablen Nutzung von KI-Systemen 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
Allgemeine Nutzung von KI	5.1, 5.2, 5.3	1.1.1, 1.2.1	6.1, 6.2, 6.3	ORP1, ORP2, ORP3	AIS-01, AIS-02	PR.AC-1, PR.AC-2	Artikel 5, 6.1	Abschnitt 2.3	Artikel 23	Artikel 4
Verantwortlicher Umgang mit KI	5.10	2.1.1, 2.1.2	5.1, 5.2	ORP4, ORP5	AIS-03	PR.AC-3, PR.AC-4	Artikel 5, 6.2	Abschnitt 2.4	Artikel 23	Artikel 4
Datenschutz bei der Nutzung von KI	5.12	3.1.1, 3.1.2	7.1, 7.2	OPS1, OPS2	DSI-01, DSI-02	PR.DS-2, PR.DS-3	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Zugangskontrollen für KI-Systeme	7.2	3.2.1, 3.2.2	8.1, 8.2	OPS3, OPS4	IAM-01, IAM-02	PR.AC-5, PR.AC-6	Artikel 6.4	Abschnitt 2.6	Artikel 23	Artikel 4
Verbotene Anwendungen von KI	5.19	4.1.1, 4.1.2	9.1, 9.2	ORP6, ORP7	AIS-04, AIS-05	PR.IP-1, PR.IP-2	Artikel 6.5	Abschnitt 2.7	Artikel 23	Artikel 4
Überwachung und Logging von KI-Aktivitäten	8.22	4.2.1, 4.2.2	10.1, 10.2	ORP8, ORP9	IVS-01, IVS-02	PR.AC-7, PR.AC-8	Artikel 6.6	Abschnitt 2.8	Artikel 23	Artikel 4
Nutzung von KI-Diensten in der Cloud	8.1, 8.2	5.1.1, 5.1.2	11.1, 11.2	PHY1, PHY2	DSI-03, DSI-04	PR.AC-9, PR.AC-10	Artikel 6.7	Abschnitt 2.9	Artikel 23	Artikel 4
Konsequenzen bei Missbrauch von KI-Systemen	5.22	5.2.1, 5.2.2	12.1, 12.2	ORP10, ORP11	GOV-01, GOV-02	PR.IP-3, PR.IP-4	Artikel 6.8	Abschnitt 2.10	Artikel 23	Artikel 4
Schulung und Sensibilisierung zur KI-Nutzung	6.7, 6.8	4.3.1, 4.3.2	13.1, 13.2	ORP12, ORP13	IAM-03, IAM-04	PR.AC-11, PR.AC-12	Artikel 6.9	Abschnitt 2.11	Artikel 24	Artikel 5

## Richtlinien und Anforderungen

### Allgemeine Nutzung von KI

Die Nutzung der KI-Ressourcen muss in Übereinstimmung mit den Prinzipien der Vertraulichkeit, Integrität und Verfügbarkeit erfolgen (ISO 27001: 5.1, 5.2, 5.3). Alle Benutzer müssen sich der Richtlinien und Verfahren zur akzeptablen Nutzung von KI bewusst sein und diese einhalten (CIS Controls 6.1, 6.2, 6.3, TISAX 1.1.1, 1.2.1). Es ist sicherzustellen, dass alle Aktivitäten protokolliert und überwacht werden, um ungewöhnliche oder unautorisierte Aktivitäten frühzeitig zu erkennen (BSI C5: ORP1, ORP2, ORP3, CCM AIS-01, AIS-02).

### Verantwortlicher Umgang mit KI

Die Nutzung von KI-Ressourcen sollte verantwortungsvoll und ethisch erfolgen (ISO 27001: 5.10). Benutzer dürfen keine KI-Systeme für schädliche oder unethische Aktivitäten einsetzen (CIS Controls 5.1, 5.2, TISAX 2.1.1, 2.1.2). Alle Nutzungen müssen den ethischen Richtlinien entsprechen und dürfen keine Risiken für die Unternehmenssicherheit darstellen (NIST CSF PR.AC-3, PR.AC-4, European CRA Artikel 23).

### **Datenschutz bei der Nutzung von KI**

Der Datenschutz muss bei der Nutzung von KI-Systemen jederzeit gewährleistet sein (ISO 27001: 5.12). Personenbezogene Daten dürfen nur in Übereinstimmung mit den Datenschutzrichtlinien des Unternehmens und den gesetzlichen Anforderungen verarbeitet werden (CIS Controls 7.1, 7.2, TISAX 3.1.1, 3.1.2). Benutzer müssen sicherstellen, dass keine unbefugten Datenzugriffe oder Datenlecks auftreten (BSI C5: OPS1, OPS2, CCM DSI-01, DSI-02).

### **Zugangskontrollen für KI-Systeme**

Der Zugang zu KI-Systemen muss strikt kontrolliert werden (ISO 27001: 7.2). Benutzer müssen sich authentifizieren und autorisieren, um Zugriff auf die KI-Ressourcen zu erhalten (CIS Controls 8.1, 8.2, TISAX 3.2.1, 3.2.2). Unbefugter Zugang muss verhindert und jegliche Sicherheitsvorfälle müssen gemeldet werden (NIST CSF PR.AC-5, PR.AC-6, NIS2 Artikel 6.4).

### **Verbotene Anwendungen von KI**

Jegliche Nutzung von KI-Systemen, die gegen gesetzliche oder ethische Vorgaben verstößt, ist verboten (ISO 27001: 5.19). Dazu gehören Anwendungen, die diskriminierend, belästigend oder schädlich sind (CIS Controls 9.1, 9.2, TISAX 4.1.1, 4.1.2). Verstöße können zu disziplinarischen Maßnahmen führen (European CRA Artikel 23, OH SZA Abschnitt 2.7).

### **Überwachung und Logging von KI-Aktivitäten**

Alle Aktivitäten auf KI-Systemen müssen überwacht und protokolliert werden (ISO 27001: 8.22). Es ist sicherzustellen, dass alle Zugriffe und Nutzungen nachvollziehbar sind und keine unautorisierten Aktivitäten stattfinden (CIS Controls 10.1, 10.2, TISAX 4.2.1, 4.2.2). Die Protokollierung muss regelmäßig überprüft und ausgewertet werden, um Sicherheitsvorfälle frühzeitig zu erkennen (NIST CSF PR.AC-7, PR.AC-8, BSI C5: ORP8, ORP9, CCM IVS-01, IVS-02).

### **Nutzung von KI-Diensten in der Cloud**

Die Nutzung von KI-Diensten in der Cloud muss sicher und kontrolliert erfolgen (ISO 27001: 8.1, 8.2). Sicherheitsmaßnahmen wie Verschlüsselung, Zugriffskontrolle und regelmäßige Sicherheitsüberprüfungen müssen implementiert werden (CIS Controls 11.1, 11.2, TISAX 5.1.1, 5.1.2). Alle Cloud-Dienste müssen den Unternehmensrichtlinien entsprechen und dürfen keine Sicherheitsrisiken darstellen (NIST CSF PR.AC-9, PR.AC-10, BSI C5: PHY1, PHY2, CCM DSI-03, DSI-04).

### **Konsequenzen bei Missbrauch von KI-Systemen**

Verstöße gegen diese Richtlinie können zu disziplinarischen Maßnahmen führen, die bis zur Beendigung des Arbeitsverhältnisses reichen können (ISO 27001: 5.22). Alle Vorfälle müssen dokumentiert und gemäß den Unternehmensrichtlinien gemeldet werden (CIS Controls 12.1, 12.2, TISAX 5.2.1, 5.2.2). Das Management ist dafür verantwortlich, geeignete Maßnahmen zu ergreifen, um Wiederholungen zu verhindern (NIST CSF PR.IP-3, PR.IP-4, BSI C5: ORP10, ORP11, CCM GOV-01, GOV-02).

### **Schulung und Sensibilisierung zur KI-Nutzung**

Alle Mitarbeiter müssen regelmäßig Schulungen zur sicheren und ethischen Nutzung von KI-Systemen durchlaufen (ISO 27001: 6.7, 6.8). Diese Schulungen müssen die Richtlinien zur Nutzung von KI sowie die potenziellen Risiken und Herausforderungen abdecken (CIS Controls 13.1, 13.2, TISAX 4.3.1, 4.3.2). Sensibilisierungsmaßnahmen müssen implementiert werden, um sicherzustellen, dass alle Mitarbeiter über die aktuellen Bedrohungen und Sicherheitsmaßnahmen informiert sind (NIST CSF PR.AC-11, PR.AC-12, BSI C5: ORP12, ORP13, CCM IAM-03, IAM-04).

### **Verantwortliche**

Die Implementierung und Einhaltung dieser Richtlinie liegt in der Verantwortung des IT-Sicherheitsbeauftragten und des Managements. 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 KI-Umgebung bei [Unternehmen].

=====

**Dokumentinformationen**

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