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 zur akzeptablen Nutzung von Unternehmenssystemen

Datum: [Heutiges Datum]

Einleitung

Diese Richtlinie zur akzeptablen Nutzung von Unternehmenssystemen definiert die Anforderungen und Maßnahmen zur Sicherstellung einer sicheren und verantwortungsvollen Nutzung der IT-Ressourcen 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 IT-Ressourcen von [Unternehmen] haben.

Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie zur akzeptablen Nutzung von Unternehmenssystemen 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	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
Persönliche Nutzung	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
E-Mail und Instant Messaging	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
Zugangskarten und Schlüssel	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 Kommunikation	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
Internetnutzung	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 Arbeitsstationen und Laptops	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 Richtlinienverstößen	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
Remote-Arbeit	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
Nutzung von Cloud-Diensten	5.23, 5.24	4.4.1, 4.4.2	14.1, 14.2	ORP14, ORP15	CSP-01, CSP-02	PR.AC-13, PR.AC-14	Artikel 7.1	Abschnitt 2.12	Artikel 25	Artikel 6
Zugriffskontrollen	8.3, 8.4, 8.5	2.2.1, 2.2.2	15.1, 15.2	ORP16, ORP17	IAM-05, IAM-06	PR.AC-15, PR.AC-16	Artikel 7.2	Abschnitt 2.13	Artikel 26	Artikel 7

Richtlinien und Anforderungen

Allgemeine Nutzung

Die Nutzung der IT-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 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).

Persönliche Nutzung

Die persönliche Nutzung der IT-Ressourcen sollte minimal sein und die beruflichen Aufgaben nicht beeinträchtigen (ISO 27001: 5.10). Benutzer dürfen keine privaten Daten auf Unternehmensressourcen speichern oder nicht autorisierte Software installieren (CIS Controls 5.1, 5.2, TISAX 2.1.1, 2.1.2). Alle persönlichen Nutzungen müssen den Sicherheitsrichtlinien entsprechen und dürfen keine Risiken für die Unternehmenssicherheit darstellen (NIST CSF PR.AC-3, PR.AC-4, European CRA Artikel 23).

E-Mail und Instant Messaging

E-Mails und Instant Messaging müssen für geschäftliche Zwecke verwendet werden und den Unternehmensrichtlinien entsprechen (ISO 27001: 5.12). Der Austausch vertraulicher Informationen über unsichere Kanäle ist untersagt (CIS Controls 7.1, 7.2, TISAX 3.1.1, 3.1.2). Benutzer müssen verdächtige E-Mails und Nachrichten umgehend dem IT-Sicherheitsteam melden (BSI C5: OPS1, OPS2, CCM DSI-01, DSI-02).

Zugangskarten und Schlüssel

Der Zugang zu physischen und virtuellen Ressourcen muss strikt kontrolliert werden (ISO 27001: 7.2). Zugangskarten und Schlüssel dürfen nicht weitergegeben oder dupliziert werden (CIS Controls 8.1, 8.2, TISAX 3.2.1, 3.2.2). Verlorene oder gestohlene Zugangsmittel müssen sofort gemeldet werden (NIST CSF PR.AC-5, PR.AC-6, NIS2 Artikel 6.4).

Verbotene Kommunikation

Jegliche Kommunikation, die illegal ist oder gegen die Unternehmensrichtlinien verstößt, ist verboten (ISO 27001: 5.19). Dazu gehören diskriminierende, belästigende oder beleidigende Inhalte (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).

Internetnutzung

Der Zugriff auf das Internet muss sicher und kontrolliert erfolgen (ISO 27001: 8.22). Das Herunterladen und Installieren von nicht autorisierter Software ist untersagt (CIS Controls 10.1, 10.2, TISAX 4.2.1, 4.2.2). Alle Internetaktivitäten müssen den Sicherheitsrichtlinien entsprechen und dürfen keine Sicherheitsrisiken darstellen (NIST CSF PR.AC-7, PR.AC-8, BSI C5: ORP8, ORP9, CCM IVS-01, IVS-02).

Nutzung von Arbeitsstationen und Laptops

Arbeitsstationen und Laptops müssen sicher konfiguriert und vor unbefugtem Zugriff geschützt werden (ISO 27001: 8.1, 8.2). Dies beinhaltet die Implementierung von Sicherheitsmaßnahmen wie Netzwerksicherheit, Zugriffskontrolle und Datensicherung (CIS Controls 11.1, 11.2, TISAX 5.1.1, 5.1.2). Regelmäßige Überprüfungen und Bewertungen der Systeme sind notwendig, um sicherzustellen, dass sie gegen aktuelle Bedrohungen geschützt sind (BSI C5: PHY1, PHY2, CCM DSI-03, DSI-04).

Konsequenzen bei Richtlinienverstößen

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).

Remote-Arbeit

Die Arbeit von entfernten Standorten muss sicher und kontrolliert erfolgen (ISO 27001: 6.7, 6.8). Sicherheitsmaßnahmen wie Netzwerksicherheit, Zugriffskontrolle und Datensicherung müssen implementiert werden, um die Integrität und Vertraulichkeit der Daten zu gewährleisten (CIS Controls 13.1, 13.2, TISAX 4.3.1, 4.3.2). Regelmäßige Überprüfungen und Bewertungen der Remote-Arbeitsplätze sind notwendig (NIST CSF PR.AC-11, PR.AC-12, BSI C5: ORP12, ORP13, CCM IAM-03, IAM-04).

Nutzung von Cloud-Diensten

Die Nutzung von Cloud-Diensten muss sicher und kontrolliert erfolgen (ISO 27001: 5.23, 5.24). Dies beinhaltet die Implementierung von Sicherheitsmaßnahmen wie Netzwerksicherheit, Zugriffskontrolle und Datensicherung (CIS Controls 14.1, 14.2, TISAX 4.4.1, 4.4.2). Regelmäßige Überprüfungen und Bewertungen der Cloud-Dienste sind notwendig, um sicherzustellen, dass sie gegen aktuelle Bedrohungen geschützt sind (NIST CSF PR.AC-13, PR.AC-14, BSI C5: ORP14, ORP15, CCM CSP-01, CSP-02).

Zugriffskontrollen

Zugriffskontrollen müssen implementiert werden, um den unbefugten Zugriff auf Unternehmensressourcen zu verhindern (ISO 27001: 8.3, 8.4, 8.5). Dies beinhaltet die Implementierung von Maßnahmen wie Authentifizierung, Autorisierung und Überwachung (CIS Controls 15.1, 15.2, TISAX 2.2.1, 2.2.2). Regelmäßige Überprüfungen und Bewertungen der Zugriffskontrollen sind notwendig (NIST CSF PR.AC-15, PR.AC-16, BSI C5: ORP16, ORP17, CCM IAM-05, IAM-06).

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	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 IT-Umgebung bei [Unternehmen].

Dokumentinformationen

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