



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 Informationsklassifizierung und -schutz

Datum: [Heutiges Datum]

Einleitung

Diese Richtlinie zur Informationsklassifizierung und -schutz definiert die Anforderungen und Maßnahmen zur Klassifizierung und zum Schutz von Informationen 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 Informationen von [Unternehmen] haben oder für deren Schutz verantwortlich sind.

Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie zur Informationsklassifizierung und -schutz 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
Klassifizierung von Informationen	8.2.1, 8.2.2	1.1.1, 1.2.1	3.1, 3.2	ORP1, ORP2	DSI-01, DSI-02	PR.IP-1, PR.IP-2	Artikel 5, 6.1	Abschnitt 2.3	Artikel 23	Artikel 4
Kennzeichnung von Informationen	8.3.1, 8.3.2	2.1.1, 2.1.2	4.1, 4.2	ORP3, ORP4	DSI-03, DSI-04	PR.IP-3, PR.IP-4	Artikel 5, 6.2	Abschnitt 2.4	Artikel 23	Artikel 4
Zugriffskontrollen	9.1.2, 9.1.3	3.1.1, 3.1.2	5.1, 5.2	OPS1, OPS2	IAM-01, IAM-02	PR.AC-1, PR.AC-2	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Schutzmaßnahmen für vertrauliche Informationen	8.4.1, 8.4.2	3.2.1, 3.2.2	6.1, 6.2	OPS3, OPS4	DSI-05, DSI-06	PR.DS-1, PR.DS-2	Artikel 6.4	Abschnitt 2.6	Artikel 23	Artikel 4
Schulung und Sensibilisierung	6.3.1, 6.3.2	4.1.1, 4.1.2	7.1, 7.2	ORP5, ORP6	STA-01, STA-02	PR.AT-1, PR.AT-2	Artikel 6.5	Abschnitt 2.7	Artikel 23	Artikel 4
Überwachung und Überprüfung	9.4.1, 9.4.2	4.2.1, 4.2.2	8.1, 8.2	ORP7, ORP8	IVS-01, IVS-02	DE.CM-1, DE.CM-2	Artikel 6.6	Abschnitt 2.8	Artikel 23	Artikel 4

Richtlinien und Anforderungen

Klassifizierung von Informationen

Alle Informationen müssen nach ihrem Schutzbedarf klassifiziert werden (ISO 27001: 8.2.1, 8.2.2). Dies umfasst die Identifizierung und Kategorisierung von Informationen basierend auf ihrer Vertraulichkeit, Integrität und Verfügbarkeit (CIS Controls 3.1, 3.2, TISAX 1.1.1, 1.2.1). Die Klassifizierung muss dokumentiert und regelmäßig überprüft werden, um sicherzustellen, dass sie den aktuellen Anforderungen entspricht (BSI C5: ORP1, ORP2, CCM DSI-01, DSI-02).

Kennzeichnung von Informationen

Alle klassifizierten Informationen müssen entsprechend ihrer Klassifizierung gekennzeichnet werden (ISO 27001: 8.3.1, 8.3.2). Dies erleichtert die Identifizierung und den Schutz der Informationen durch entsprechende Maßnahmen (CIS Controls 4.1, 4.2, TISAX 2.1.1, 2.1.2). Die Kennzeichnung muss deutlich und konsistent erfolgen, um Missverständnisse zu vermeiden (BSI C5: ORP3, ORP4, CCM DSI-03, DSI-04).

Zugriffskontrollen

Der Zugang zu klassifizierten Informationen muss strikt kontrolliert werden (ISO 27001: 9.1.2, 9.1.3). Dies umfasst die Implementierung von Zugriffskontrollen und Authentifizierungsmechanismen, um unbefugten Zugriff zu verhindern (CIS Controls 5.1, 5.2, TISAX 3.1.1, 3.1.2). Regelmäßige Überprüfungen der Zugriffskontrollen sind notwendig, um die Sicherheit der Informationen zu gewährleisten (NIST CSF PR.AC-1, PR.AC-2, BSI C5: OPS1, OPS2, CCM IAM-01, IAM-02).

Schutzmaßnahmen für vertrauliche Informationen

Vertrauliche Informationen müssen durch geeignete Schutzmaßnahmen gesichert werden (ISO 27001: 8.4.1, 8.4.2). Dies umfasst die Nutzung von Verschlüsselung, sichere Aufbewahrung und die Implementierung von Sicherheitsmaßnahmen für die Übertragung von Daten (CIS Controls 6.1, 6.2, TISAX 3.2.1, 3.2.2). Regelmäßige Sicherheitsüberprüfungen sind notwendig, um die Einhaltung der Schutzmaßnahmen sicherzustellen (NIST CSF PR.DS-1, PR.DS-2, BSI C5: OPS3, OPS4, CCM DSI-05, DSI-06).

Schulung und Sensibilisierung

Alle Mitarbeiter müssen regelmäßig Schulungen zur Informationsklassifizierung und -schutz durchlaufen (ISO 27001: 6.3.1, 6.3.2). Diese Schulungen müssen die aktuellen Bedrohungen, Sicherheitsmaßnahmen und Best Practices abdecken (CIS Controls 7.1, 7.2, TISAX 4.1.1, 4.1.2). 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).

Überwachung und Überprüfung

Alle Maßnahmen zur Informationsklassifizierung und -schutz müssen regelmäßig überwacht und überprüft werden (ISO 27001: 9.4.1, 9.4.2). Die Ergebnisse der Überwachung müssen dokumentiert und analysiert werden, um Verbesserungspotenziale zu identifizieren und die Einhaltung der Richtlinien sicherzustellen (CIS Controls 8.1, 8.2, TISAX 4.2.1, 4.2.2). Regelmäßige Audits sind notwendig, um die Wirksamkeit der Maßnahmen zu bewerten (NIST CSF DE.CM-1, DE.CM-2, BSI C5: ORP7, ORP8, CCM IVS-01, IVS-02).

Verantwortliche

Die Implementierung und Einhaltung dieser Richtlinie liegt in der Verantwortung des IT-Sicherheitsbeauftragten und des Information Security 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 Informationsklassifizierung und -schutz bei [Unternehmen].

Dokumentinformationen

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

