

Author	Dipl.-Ing. Daniel Mrskos, BSc
Funktion	CEO von Security mit Passion, Penetration Tester, Mentor, FH-Lektor, NIS Prüfer
Datum	04. Juli 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

Anleitung zur Nutzung der Prozessbeschreibungen

Einleitung

Diese Prozessbeschreibungen dienen als Basis für alle, die Prozessbeschreibungen zur Erfüllung von Compliance-Anforderungen und gesetzlichen Vorgaben implementieren möchten oder müssen. Die nachfolgenden Normen und Standards wurden als Grundlage für die Erstellung dieser Policies herangezogen:

- ISO 27001:2022
- COBIT
- ITIL

Prozessbeschreibungen bearbeiten

Im Ordner "Source" befinden sich alle .md-Dateien (Markdown), die sowohl mittels Copy-

Paste in einem "What You See Is What You Get" (WYSIWYG) Editor wie beispielsweise von Confluence oder ähnlichen Tools kopiert werden können, als auch mittels Markdown-Editor als PDF kompiliert werden können. Security mit Passion hat für die Erstellung dieser Dokumente [Macdown](#) benutzt.

01_Prozessbeschreibung- Erstellung und Pflege der IT-Sicherheitsleitlinie.md

Practices.

- 3. Erstellung der IT-Sicherheitsleitlinie**
 - Verantwortlich: IT-Sicherheitsbeauftragter
 - Beschreibung: Erstellung des Entwurfs der IT-Sicherheitsleitlinie unter Berücksichtigung der erhobenen Anforderungen und unter Einbindung aller relevanten Abteilungen.
- 4. Überprüfung und Freigabe**
 - Verantwortlich: Geschäftsführung, Compliance-Abteilung
 - Beschreibung: Prüfung des Entwurfs auf Vollständigkeit und Konformität. Freigabe durch die Geschäftsführung.
- 5. Kommunikation und Schulung**
 - Verantwortlich: Personalabteilung, IT-Abteilung
 - Beschreibung: Veröffentlichung der IT-Sicherheitsleitlinie und Durchführung von Schulungen für alle Mitarbeiter.
- 6. Kontinuierliche Überprüfung und Aktualisierung**
 - Verantwortlich: IT-Sicherheitsbeauftragter
 - Beschreibung: Regelmäßige Überprüfung der IT-Sicherheitsleitlinie (mindestens jährlich) sowie anlassbezogen bei neuen Bedrohungen oder Änderungen in den regulatorischen Anforderungen. Dokumentation und Umsetzung von Änderungen.

```

```

Dokumentation

Alle Schritte und Entscheidungen im Prozess werden dokumentiert und revisionssicher archiviert. Dazu gehören:

- Entwurfsversionen der IT-Sicherheitsleitlinie
- Prüfergebnisse und Freigaben
- Schulungsunterlagen und Teilnehmerlisten
- Protokolle der Überprüfungen und Aktualisierungen

Es empfiehlt sich, die .md-Dateien mit einem Markdown-Editor auf die spezifischen Anforderungen und Bedürfnisse der eigenen Firma anzupassen, um sicherzustellen, dass sie den individuellen Sicherheits- und Compliance-Anforderungen gerecht werden.

Haftungsausschluss

Weder die Firma Security mit Passion noch der Autor Dipl.-Ing Daniel Mrskos, BSc haften für die Korrektheit oder Ausführlichkeit dieser Prozessbeschreibungen. Die bereitgestellten Prozessbeschreibungen dienen lediglich als Orientierung und sollten individuell auf die spezifischen Anforderungen und Rahmenbedingungen des jeweiligen Unternehmens angepasst werden.

Quellen und Referenzen

Quelle	Zweck	Link
ISO27001:2022	Aufbau und Implementierung eines ISMS	<u>ISO 27001:2022</u>
COBIT	Control Objectives for Information and Related Technology	<u>COBIT</u>
ITIL	Information Technology Infrastructure Library	<u>ITIL</u>