\*\* KOSTENLOSE VORSCHAU \*\*

[Logo der Organisation]

[Name der Organisation]

**ERKLÄRUNG ZUR ANWENDBARKEIT**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Datum der Version: |  |
| Erstellt durch: |  |
| Genehmigt durch: |  |
| Vertraulichkeitsstufe: |  |

**Änderungs-Historie**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Version** | **Erstellt durch** | **Beschreibung der Änderung** |
|  | 0.1 | 27001Academy | Erster Entwurf des Dokuments |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Inhaltsverzeichnis**

[1. Zweck, Anwendungsbereich und Anwender 3](#_Toc37064201)

[2. Referenzdokumente 3](#_Toc37064202)

[3. Anwendbarkeit von Maßnahmen 3](#_Toc37064203)

[4. Akzeptanz von Restrisiken 18](#_Toc37064204)

[5. Gültigkeit und Dokumenten-Handhabung 19](#_Toc37064205)

# Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Dokuments ist die Definition, welche Maßnahmen zur Umsetzung in [Name der Organisation] geeignet sind, welches die Maßnahmenziele sind, wie diese umgesetzt werden, sowie die Genehmigung von Restrisiken und die formale Genehmigung der Umsetzung genannter Maßnahmen.

Dieses Dokument beinhaltet alle Maßnahmen, die in Anhang A der ISO 27001 Norm aufgeführt sind. Die Maßnahmen sind auf den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems anzuwenden.

Anwender dieses Dokuments sind alle Mitarbeiter von [Name der Organisation] mit einer Funktion im ISMS.

# Referenzdokumente

* ISO/IEC 27001 Norm, Abschnitt 6.1.3 d)
* Informationssicherheitspolitik
* Methodik zur Risikoeinschätzung und Risikobehandlung
* Bericht zur Risikoeinschätzung und Risikobehandlung

# Anwendbarkeit von Maßnahmen

Die folgenden Maßnahmen aus ISO 27001 Anhang A sind anwendbar:

| ID | Maßnahmen gemäß ISO/IEC 27001 | Anwend-barkeit (JA/  NEIN) | … | … | Umsetzungs-methode | … |
| --- | --- | --- | --- | --- | --- | --- |
| A.5 | Sicherheitspolitik |  |  |  |  |  |
| A.5.1 | Management-Leitlinien zur Informationssicherheit |  |  |  |  |  |
| A.5.1.1 | Informationssicherheits-politik |  |  |  | Alle Richtlinien, auf die in dieser Spalte nachstehend hingewiesen wird. |  |
| A.5.1.2 | Überprüfung der Informationssicherheits-politik |  |  |  | Jede Richtlinie mit einem designierten Eigentümer, welcher das Dokument in vorgeplanten Intervallen zu überprüfen hat. |  |
| A.6 | Organisation der Informationssicherheit |  |  |  |  |  |
| A.6.1 | Interne Organisation |  |  |  |  |  |
| A.6.1.1 | Rollen und Verantwortlichkeiten im Rahmen der Informationssicherheit |  |  |  | Die Verant-wortlichkeiten für Informations-sicherheit sind in verschiedenen ISMS-Dokumenten aufgeführt. Falls erforderlich, legt [Stellenbezeich-nung] zusätzliche Verantwortlich-keiten fest. |  |
| A.6.1.2 | Pflichtentrennung |  |  |  | Jede Tätigkeit, welche der Handhabung sensibler Informationen bedarf, wird von einer Person genehmigt und von einer anderen Person ausgeführt. |  |
| A.6.1.3 | Kontakthaltung mit Behörden |  |  |  | [Betriebliche Kontinuitätsstrategie], [Vorfallreaktionsplan] |  |
| A.6.1.4 | Kontakthaltung mit besonderen Interessengruppen |  |  |  | [Stellenbezeichnung] ist verantwortlich für die Überwachung von [Interessengruppen und Sicherheits-Foren hier auflisten] |  |

\*\* ENDE DER KOSTENLOSEN VORSCHAU \*\*

Um dieses Dokument vollständig herunterzuladen, klicken Sie bitte hier:  
<https://advisera.com/27001academy/de/documentation/erklaerung-zur-anwendbarkeit/>