\*\*KOSTENLOSE VORSCHAUVERSION\*\*

[Logo der Organisation]

[Name der Organisation]

**RICHTLINIE ZUR ENTWICKLUNGSSICHERHEIT**

|  |  |
| --- | --- |
| 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

2. Referenzdokumente 3

3. Sichere Entwicklung und Wartung 3

3.1. Risikoeinschätzung beim Entwicklungsprozess 3

3.2. Sicherung des Entwicklungsumfeldes 3

3.3. Grundsätze für das Engineering sicherer Systeme 3

3.4. Sichere Kodierung 4

3.5. Sicherheitsanforderungen 4

3.6. Sicherheitsanforderungen im Zusammenhang mit öffentlichen Netzwerken 4

3.7. Prüfung und Testung der Umsetzung von Sicherheitsanforderungen 4

3.8. Verwahrungsort 5

3.9. Verwaltung von Versionen 5

3.10. Verwaltung von Änderungen 5

3.11. Schutz von Testdaten 5

3.12. Erforderliches Sicherheitstraining 5

4. Verwaltung von Aufzeichnungen zu diesem Dokument 5

5. Gültigkeit und Dokumenten-Handhabung 6

6. Anhänge 6

# Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Dokuments ist die Festlegung grundsätzlicher Vorschriften bei der sicheren Entwicklung von Software und Systemen.

Dieses Dokument gilt für die Entwicklung und Wartung sämtlicher Dienstleistungen, Architektur, Software und Systeme, die Teil des Informationssicherheits-Managementsystems (ISMS) sind.

Anwender dieses Dokuments sind alle bei [Name der Organisation] in der Entwicklung und Wartung eingesetzten Mitarbeiter.

# Referenzdokumente

* ISO/IEC 27001 Norm, Abschnitte A.5.33, A.8.11, A.8.25, A.8.26, A.8.27, A.8.28, A.8.29, A.8.30, A.8.31, A.8.32 und A.8.33
* Methodik zur Risikoeinschätzung und Risikobehandlung
* Sicherheitspolitik für Lieferanten
* [Richtlinie zum Änderungsmanagement] / [Sicherheitsverfahren für die IT-Abteilung]
* Plan für Training und Awareness

# Sichere Entwicklung und Wartung

## Risikoeinschätzung beim Entwicklungsprozess

Zusätzlich zu der gemäß der Methodik zur Risikoeinschätzung und –Behandlung durchgeführten Risikoeinschätzung muss [Stellenbezeichnung] auch regelmäßig eine Einschätzung des folgenden durchführen:

* Risiken im Zusammenhang mit unerlaubtem Zugang zum Entwicklungsumfeld
* Risiken im Zusammenhang mit unerlaubten Änderungen am Entwicklungsumfeld
* Technische Schwachstellen der in der Organisation benutzten IT-Systeme
* Mögliche Risiken, die eine neue Technologie bringen könnte, wenn sie in der Organisation eingeführt und benutzt wird
* Risiken, die eine neue Entwicklungsmethodik und/oder Programmiersprache mit sich bringen kann, wenn sie im Unternehmen eingesetzt wird
* Risiken im Zusammenhang mit den Lizenzierungsanforderungen

\*\*ENDE DER KOSTENFREIEN VORSCHAU\*\*

Um die Vollversion dieses Dokumentes herunterzuladen, klicken Sie hier:

<https://advisera.com/27001academy/de/documentation/richtlinie-zur-entwicklungssicherheit/>