\*\*KOSTENLOSE VORSCHAUVERSION\*\*

[Logo der Organisation]

[Name der Organisation]

**RICHTLINIE ZUR KLASSIFIZIERUNG VON INFORMATIONEN**

|  |  |
| --- | --- |
| 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. Klassifizierte Information 3

3.1. Umsetzungsschritte und Verantwortlichkeiten 3

3.2. Klassifizierung von Information 4

3.2.1. Klassifizierungskriterien 4

3.2.2. Vertraulichkeitsstufen 4

3.2.3. Liste berechtigter Personen 5

3.2.4. Re-Klassifizierung 5

3.3. Kennzeichnung von Information 5

3.4. Umgang mit klassifizierter Information 5

3.5. Datenmaskierung 9

4. Verwaltung von Aufzeichnungen zu diesem Dokument 10

5. Gültigkeit und Dokumenten-Handhabung 10

# Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Dokuments ist sicherzustellen, dass Informationen auf einem angemessenen Niveau geschützt sind.

Dieses Dokument gilt für den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS), d.h. für alle Arten von Information, unabhängig von deren Form – Papier oder elektronische Dokumente, Anwendungen und Datenbanken, persönliches Wissen, etc.

Anwender dieses Dokuments sind alle Mitarbeiter von [Name der Organisation].

# Referenzdokumente

* ISO/IEC 27001 Norm, Abschnitte A.5.9, A.5.10, A.5.12, A.5.13, A.5.14, A.7.10, A.8.3, A.8.5, A.8.11 und A.8.12
* Informationssicherheitspolitik
* Bericht zur Risikoeinschätzung und Risikobehandlung
* Erklärung zur Anwendbarkeit
* Inventar der Werte
* Liste gesetzlicher, amtlicher, vertraglicher und anderer Verpflichtungen
* Verfahren zum Vorfallmanagement
* [Sicherheitsverfahren für die IT-Abteilung] / [Richtlinie zu Entsorgung und Vernichtung]
* IT-Sicherheitspolitik

# Klassifizierte Information

## Umsetzungsschritte und Verantwortlichkeiten

Folgendes sind die Umsetzungsschritte und Verantwortlichkeiten für Informationsmanagement:

|  |  |
| --- | --- |
| ***Bezeichnung des Umsetzungsschrittes*** | ***Verantwortlichkeit*** |
| 1. Eintrag des Informationswertes in das Inventar der Werte | [Stellenbezeichnung] |
| 2. Klassifizierung der Information | Eigentümer des Wertes |
| 3. Kennzeichnung der Information | Eigentümer des Wertes |
| 4. Verwaltung der Information | Personen mit Benutzerberechtigung entsprechend dieser Richtlinie |

Falls klassifizierte Informationen von außerhalb der Organisation empfangen werden, ist [Stellenbezeichnung] für deren Klassifizierung entsprechend der Vorgaben dieser Richtlinie verantwortlich und diese Person wird zum Eigentümer dieses Informationswertes.

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

Um die Vollversion dieses Dokumentes herunterzuladen, klicken Sie hier:

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