\*\* KOSTENLOSE VORSCHAU \*\*

[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](#_Toc490138568)

[2. Referenzdokumente 3](#_Toc490138569)

[3. Klassifizierte Information 3](#_Toc490138570)

[3.1. Umsetzungsschritte und Verantwortlichkeiten 3](#_Toc490138571)

[3.2. Klassifizierung von Information 4](#_Toc490138572)

[3.2.1. Klassifizierungskriterien 4](#_Toc490138573)

[3.2.2. Vertraulichkeitsstufen 4](#_Toc490138574)

[3.2.3. Liste berechtigter Personen 5](#_Toc490138575)

[3.2.4. Re-Klassifizierung 5](#_Toc490138576)

[3.3. Kennzeichnung von Information 5](#_Toc490138577)

[3.4. Umgang mit klassifizierter Information 5](#_Toc490138578)

[4. Verwaltung von Aufzeichnungen die zu diesem Dokument erstellt wurden 9](#_Toc490138579)

[5. Gültigkeit und Dokumenten-Handhabung 9](#_Toc490138580)

# 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.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3
* Informationssicherheitspolitik
* Bericht zur Risikoeinschätzung und Risikobehandlung
* Erklärung zur Anwendbarkeit
* Inventar der Werte
* Liste gesetzlicher, amtlicher, vertraglicher und anderer Verpflichtungen
* Verfahren zum Umgang mit Informationssicherheits-Vorfällen
* [Sicherheitsverfahren für die IT-Abteilung] / [Richtlinie zu Entsorgung, Vernichtung und Weiterverwendung]
* 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.

## Klassifizierung von Information

### Klassifizierungskriterien

Die Vertraulichkeitsstufe wird auf Basis folgender Kriterien festgelegt:

* Wert der Information – basierend auf den in der Risikoeinschätzung festgestellten Auswirkungen
* …

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

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