\*\* 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** |
| TT.MM.JJJJ | 0.1 | EUGDPRAcademy | Erster Entwurf des Dokuments |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Inhaltsverzeichnis**

[1. Zweck, Anwendungsbereich und Anwender 3](#_Toc505026900)

[2. Referenzdokumente 3](#_Toc505026901)

[3. Klassifizierte Information 3](#_Toc505026902)

[3.1. Umsetzungsschritte und Verantwortlichkeiten 3](#_Toc505026903)

[3.2. Klassifizierung von Information 4](#_Toc505026904)

[3.2.1. Klassifizierungskriterien 4](#_Toc505026905)

[3.2.2. Vertraulichkeitsstufen 4](#_Toc505026906)

[3.2.3. Liste berechtigter Personen 5](#_Toc505026907)

[3.2.4. Re-Klassifizierung 5](#_Toc505026908)

[3.3. Kennzeichnung von Information 5](#_Toc505026909)

[3.4. Umgang mit klassifizierter Information 5](#_Toc505026910)

[4. Verwaltung von Aufzeichnungen die zu diesem Dokument erstellt wurden 9](#_Toc505026911)

[5. Gültigkeit und Dokumenten-Handhabung 9](#_Toc505026912)

# 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 (einschließlich personenbezogener Daten), 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
* Reaktion auf eine Datenschutzverletzung und Meldeverfahren
* [Sicherheitsverfahren der IT-Abteilung] / [Politik zur 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.

## Klassifizierung von Information

### Klassifizierungskriterien

Die Vertraulichkeitsstufe wird auf Basis folgender Kriterien festgelegt:

* Wert der Information – basierend auf den in der Risikoeinschätzung festgestellten Auswirkungen
* Sensibilität und Kritikalität der Information – basierend auf dem für jede Information während der Risikoeinschätzung kalkulierten höchsten Risiko

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

Um dieses Dokument vollständig herunterzuladen, klicken Sie bitte hier:  
<https://advisera.com/eugdpracademy/de/documentation/richtlinie-zur-klassifizierung-von-informationen/>