\*\* KOSTENLOSE VORSCHAU \*\*

[Logo der Organisation]

[Name der Organisation]

**SICHERHEITSVERFAHREN FÜR DIE IT-ABTEILUNG**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Datum der Version: |  |
| Erstellt von: |  |
| Genehmigt von: |  |
| 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](#_Toc505066060)

[2. Referenzdokumente 3](#_Toc505066061)

[3. Sicherheitsverfahren 3](#_Toc505066062)

[3.1. Änderungsmanagement 3](#_Toc505066063)

[3.2. Backup 3](#_Toc505066064)

[3.2.1. Backup-Prozess 4](#_Toc505066065)

[3.2.2. Test von Backup-Kopien 4](#_Toc505066066)

[3.3. Management der Netzsicherheit 4](#_Toc505066067)

[3.4. Netzwerkdienste 5](#_Toc505066068)

[3.5. Entsorgung und Vernichtung von Ausstattung und Datenträgern 5](#_Toc505066069)

[3.5.1. Gerätschaften 5](#_Toc505066070)

[3.5.2. Tragbare Speichermedien 5](#_Toc505066071)

[3.5.3. Papier-Datenträger 5](#_Toc505066072)

[3.5.4. Löschungs- und Vernichtungsprotokolle; Ausschuss für die Vernichtung von Daten 5](#_Toc505066073)

[3.6. Systemüberwachung 6](#_Toc505066074)

[4. Verwaltung von Aufzeichnungen, die zu diesem Dokuments erstellt wurden 6](#_Toc505066075)

[5. Gültigkeit und Dokumentenmanagement 7](#_Toc505066076)

# Zweck, Anwendungsbereich und Anwender

Zweck dieses Dokuments ist es sicherzustellen, dass Informations- und Kommunikations-Technologie ordnungsgemäß und sicher funktioniert.

Dieses Dokument gilt für den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS) und für alle Verarbeitungstätigkeiten von personenbezogenen Daten.

Anwender dieses Dokuments sind Mitarbeiter von [Organisationseinheiten für Informations- und Kommunikations-Technologie].

# Referenzdokumente

* ISO/IEC 27001 Norm, Abschnitte A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4
* EU DSGVO Artikel 32
* Informationssicherheitspolitik
* [Richtlinie zu Mobilgeräten und Telearbeit]
* [Richtlinie zur Klassifizierung von Informationen]
* [Inventar der Werte]
* [Sicherheitspolitik für Lieferanten]

# Sicherheitsverfahren

## Änderungsmanagement

Jede Änderung an einem betrieblichen oder Produktiv-System muss wie folgt durchgeführt werden:

1. Die Änderung kann von [Stellenfunktionen angeben] beantragt werden
2. Die Änderung muss von [Stellenbezeichnung] genehmigt werden, der die Notwendigkeit dafür anhand der Geschäftsauswirkungen und potentiell negativen Auswirkungen auf die Sicherheit bewerten muss
3. Änderungen müssen von [Stellenbezeichnung] umgesetzt werden
4. [Stellenbezeichnung] ist dafür verantwortlich zu prüfen, ob die Änderung in Übereinstimmung mit der Anforderung umgesetzt wurde
5. [Stellenbezeichnung] ist für das Testen und Prüfen der Systemstabilität verantwortlich – das System darf nicht betrieben werden, bevor ausführliche Tests durchgeführt wurden
6. Die Durchführung von Änderungen muss folgenden Personen mitgeteilt werden: [hier alle notwendigen Stellenbezeichnungen auflisten]

Änderungsprotokolle werden wie folgt aufbewahrt: [Bezeichnung für das Formular angeben oder eine andere Methode für das Protokollieren von Änderungen angeben]

## Backup

### Backup-Prozess

Backup Kopien müssen erstellt werden für [bestimmen Sie die Systeme] in der Häufigkeit [bestimmen Sie die Häufigkeit].

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

Um dieses Dokument vollständig herunterzuladen, klicken Sie bitte hier:  
<https://advisera.com/eugdpracademy/de/documentation/sicherheitsverfahren-fur-die-it-abteilung/>