\*\*KOSTENLOSE VORSCHAUVERSION\*\*

[Logo der Organisation]

[Name der Organisation]

**SICHERHEITSVERFAHREN FÜR DIE IT-ABTEILUNG**

|  |  |
| --- | --- |
| 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 4

2. Referenzdokumente 4

3. Betriebsverfahren für Informations- und Kommunikationstechnik 4

3.1. Änderungsmanagement 4

3.2. Konfigurationsmanagement 5

3.3. Kapazitätsmanagement 5

3.4. Virenschutz 5

3.5. Backup 5

3.5.1. Backup-Prozess 5

3.5.2. Test von Backup-Kopien 5

3.6. Management der Netzsicherheit 6

3.7. Netzwerkdienste 6

3.8. Datenlöschung 6

3.9. Entsorgung und Vernichtung von Ausstattung und Datenträgern 7

3.9.1. Gerätschaften 7

3.9.2. Tragbare Speichermedien 7

3.9.3. Papier-Datenträger 7

3.9.4. Löschungs- und Vernichtungsprotokolle; Ausschuss für die Vernichtung von Daten 7

3.10. Informationsübertragung 8

3.10.1. Elektronische Kommunikationswege 8

3.10.2. Beziehungen zu externen Parteien 8

3.11. Umgang mit dem Quellcode 8

3.12. Verwendung von Dienstprogrammen 9

3.13. Systemüberwachung 9

3.14. Überwachung externer Bedrohungen 9

4. Verwaltung von Aufzeichnungen zu diesem Dokument 9

5. Gültigkeit und Dokumenten-Handhabung 11

# 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), d.h. für die gesamte Informations- und Kommunikations-Technologie sowie die verwandte Dokumentation innerhalb des Anwendungsbereiches.

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

# Referenzdokumente

* ISO/IEC 27001 Norm, Abschnitte A.5.7, A.5.14, A.5.37, A.7.10, A.7.14, A.8.4, A.8.6, A.8.7, A.8.8, A.8.9, A.8.10, A.8.12, A.8.13, A.8.15, A.8.16, A.8.17, A.8.18, A.8.20, A.8.21, A.8.22, A.8.23, A.8.31 und A.8.32
* Informationssicherheitspolitik
* [Notfallwiederherstellungsplan]
* [Richtlinie zu Mobilgeräten, Telearbeit und zur von zu Hause aus Arbeit]
* [Richtlinie zur Klassifizierung von Informationen]
* [Inventar der Werte]
* [Sicherheitspolitik für Lieferanten]
* [Richtlinie zur Entwicklungssicherheit]
* [Zugangssteuerungsrichtlinie]

# Betriebsverfahren für Informations- und Kommunikationstechnik

## 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]
7. [Stellenbezeichnung] ist verantwortlich für die Aktualisierung der Dokumente (Richtlinien, Verfahren, Pläne usw.), die von der Änderung betroffen sind.

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

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

Um die Vollversion dieses Dokumentes herunterzuladen, klicken Sie hier:

<https://advisera.com/27001academy/de/documentation/sicherheitsverfahren-fuer-die-it-abteilung/>