\*\*KOSTENLOSE VORSCHAUVERSION\*\*

[Logo der Organisation]

[Name der Organisation]

**IT-SICHERHEITSPOLITIK**

|  |  |
| --- | --- |
| 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. Zulässiger Gebrauch von Informationswerten 4

3.1. Definitionen 4

3.2. Zulässiger Gebrauch 4

3.3. Verantwortlichkeiten für Werte 4

3.4. Löschung von Informationen 5

3.5. Untersagte Aktivitäten 5

3.6. Entfernung von Werten aus dem Standort 5

3.7. Rückgabe von Werten bei Beendigung eines Vertrages 5

3.8. Backup-Verfahren 5

3.9. Schutz vor Viren/Malware 5

3.10. Berechtigungen zur Nutzung von Informationssystemen 6

3.11. Benutzerkonto Verantwortlichkeiten 6

3.12. Kennwort Verantwortlichkeiten 6

3.13. Richtlinie zum aufgeräumten Arbeitsplatz und leeren Bildschirm 7

3.13.1. Richtlinie zum aufgeräumten Arbeitsplatz 7

3.13.2. Richtlinie zum leeren Bildschirm 7

3.13.3. Schutz gemeinsam genutzter Einrichtungen und Gerätschaften 7

3.14. Internetnutzung 8

3.15. E-Mail und andere Verfahren für den Nachrichtenaustausch 8

3.16. Urheberrecht 9

3.17. Mobile Computing 9

3.17.1. Einleitung 9

3.17.2. Grundsätzliche Regeln 9

3.18. Telearbeit & von zu Hause aus arbeiten 10

3.18.1. Einführung 10

3.18.2. Zusätzliche Regeln für Telearbeit 10

3.19. Überwachung der Nutzung von Informations- und Kommunikationssystemen 11

3.20. Vorfälle 11

4. Verwaltung von Aufzeichnungen zu diesem Dokument 11

5. Gültigkeit und Dokumenten-Handhabung 13

# Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Dokuments ist die Festlegung klarer Regeln für den zulässigen Gebrauch von Informationssystemen und anderer Informationswerte bei [Name der Organisation].

Dieses Dokument gilt für den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS), d.h. für alle Informationssysteme und andere Informationswerte innerhalb des ISMS Anwendungsbereiches.

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

# Referenzdokumente

* ISO/IEC 27001 Norm, Abschnitte A.5.9, A.5.10, A.5.11, A.5.14, A.5.17, A.5.32, A.6.7, A.7.7, A.7.9, A.7.10, A.8.1, A.8.7, A.8.10, A.8.12, A.8.13, A.8.19, und A.8.23
* Informationssicherheitspolitik
* [Richtlinie zur Klassifizierung von Informationen]
* [Verfahren zum Vorfallmanagement]
* [Inventar der Werte]
* [Sicherheitsverfahren für die IT-Abteilung]
* [Richtlinie zur Informationsübertragung]

# Zulässiger Gebrauch von Informationswerten

## Definitionen

Informationssystem – schließt alle Server und Arbeitsplatzrechner, Netzwerk-Infrastruktur, Systemprogramme und Applikationen, Daten, sowie andere Rechner-Subsysteme und Komponenten ein, die sich im Besitz der Organisation befinden, durch die Organisation genutzt werden oder die in den Verantwortungsbereich der Organisation fallen. Der Gebrauch eines Informationssystems umfasst ebenso die Nutzung aller internen oder externen Dienste wie Internetzugang, E-Mail, usw.

Informationswerte – im Rahmen dieser Richtlinie wird der Begriff Informationswerte auf Informationssysteme und andere Informationen/Betriebsmittel, einschließlich Papierdokumente, Mobiltelefone, tragbare Computer, Speichermedien, usw. angewendet.

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

Um die Vollversion dieses Dokumentes herunterzuladen, klicken Sie hier:

<https://advisera.com/27001academy/de/documentation/it-sicherheitspolitik/>