# Die Sicherheitsleitlinie[1]

Bundesamt für Sicherheit in der Informationstechnik

Die Leitlinie zur Informationssicherheit ist ein wichtiges **Grundsatzdokument der Leitung** zu dem Stellenwert, den verbindlichen Prinzipien und dem anzustrebenden Niveau der Informationssicherheit in einer Institution. Für die betroffenen Mitarbeiter verständlich, wird auf wenigen Seiten beschrieben, welche Sicherheitsziele angestrebt und in welchem organisatorischen Rahmen diese umgesetzt werden sollen. Die Entwicklung der Leitlinie muss von der Leitung der Institution angestoßen und aktiv begleitet werden. Der ISB wird die Leitlinie in enger Kooperation mit der Leitung erarbeiten und dabei (sofern vorhanden) vom IS-Management-Team und weiteren Verantwortlichen für Informationssicherheit unterstützt.

Die Leitlinie muss **allen betroffenen Mitarbeitern bekannt gegeben** und **kontinuierlich aktualisiert** werden.

Was sollte in der Leitlinie zur Informationssicherheit festgelegt werden?

- In der Informationssicherheitsleitlinie muss beschrieben werden, für welche Bereiche diese gelten soll. Der Geltungsbereich kann die gesamte Institution umfassen oder aus Teilbereichen dieser bestehen. Wichtig ist jedoch dabei, dass die betrachteten Geschäftsaufgaben und -prozessen dem Geltungsbereich komplett enthalten sind.
- Die Bedeutung, die Informationssicherheit für eine Institution hat, wird hervorgehoben, etwa indem darauf hingewiesen wird, dass ein Ausfall der Informationstechnik oder Verletzungen der Vertraulichkeit und Integrität von Informationen die Existenz der Institution gefährden.
- Die Verantwortung der Leitung wird betont, sowohl im Hinblick auf die Initiierung des Sicherheitsprozesses als auch auf dessen kontinuierliche Verbesserung.
- Es wird auf einschlägige Gesetze und Regulierungsauflagen hingewiesen und die Mitarbeiter werden verpflichtet, diese zu beachten.
- Es werden für die Informationssicherheit besonders wichtige Geschäftsprozesse genannt, etwa Produktionsabläufe, Forschungsverfahren oder Personalbearbeitung, und auf die strikte Einhaltung von Sicherheitsregeln hingewiesen.

[1] Quelle: Online-Kurs IT-Grundschutz, Stand 07.08.2018

- Die Organisationsstruktur für Informationssicherheit und die Aufgaben der verschiedenen Sicherheitsverantwortlichen werden vorgestellt.
- Sinnvoll ist auch der Hinweis auf Sicherheitsschulungen und Sensibilisierungsmaßnahmen.

## Arbeitsauftrag zur Leitlinie

### Erstellen einer Sicherheitsleitlinie

**Aufgabenstellung für die einzelnen Gruppen!**

- **Bilden** Sie **3er** Gruppen!
- **Informieren** Sie sich über den Aufbau einer **Sicherheitsleitlinie**!
- **Verwenden** Sie dazu den **Informationstext** in **„IT10_LF4_Leitlinie“**!
- **Bearbeiten** Sie den **Arbeitsauftrag** (Seite 2) auf dem **Informationstext**!
  - **Tipp:** Das Dokument **„IT10_LF4_Beispiel_Leitlinie“** hilft Ihnen dabei!
- **Laden** Sie Ihr Dokument in den **Ordner** „06_Ergebnisse_Leitlinie“ hoch!
- **Präsentieren** Sie nach der Bearbeitungszeit Ihre Ergebnisse!

Bearbeitungszeit: **30 Minuten!**

- **Beantworten** Sie in der Gruppe **schriftlich** die folgenden Fragen (Seite 3) mit dem **Word-Dokument „Fragen zur Leitlinie…Vorlage“**.
- **Kopieren** Sie sich die Vorlage und **benennen** Sie diese entsprechend Ihres zugeteilten Gruppennamens **um**!

Hinweis: Die Beispiel Leitlinie der Recplast GmbH dient als Orientierungshilfe!

- **Erläutern Sie, warum die Leitlinie für das Krankenhaus von enormer Bedeutung ist!**
- **Beschreiben Sie, was unter dem Geltungsbereich zu verstehen ist!**
- **Beschreiben Sie den zentralen Geschäftsprozess der Abrechnungsabteilung!**
- **Formulieren Sie drei Ziele, die das Krankenhaus in der Leitlinie aufführen sollte!**
- **Wer ist trägt die Gesamtverantwortung im Krankenhaus?**
- **Welche konkreten Verantwortlichkeiten werden dem IS-Management-Team vom Vorstand übertragen?**
- **Nennen Sie zwei konkrete Aufgaben des Informationssicherheitsbeauftragten (ISB), die ihm von der Leitungsebene übertragen werden sollen!**
- **Beschreiben Sie, wie sich die Mitarbeiter im Krankenhaus verhalten müssen!**
- **Nennen Sie mindestens zwei mögliche Folgen für das Krankenhaus bei der Missachtung von Sicherheitsregeln!**
- **Nennen Sie drei Konsequenzen bei Missachtung der der Sicherheitsvorgaben!**
- **Beschreiben Sie zwei Verhaltensweisen, die zwingend zu einer Abmahnung führen!**
- **Beschreiben Sie drei grob fahrlässige Handlungen, die gegen die Sicherheitsvorgaben verstoßen und zu einer fristlosen Kündigung führen.**