

# UNTERNEHMENS IT-SECURITY RICHTLINIE



## WIESO, WESHALB, WARUM

Mitarbeiter agieren, in Bezug auf elektronische Datenverarbeitung, im Rahmen ihres eigenen Verständnisses und Ermessen. Fehlt eine klare Richtlinie zur Informationssicherheit ist die Frage einer möglichen Verantwortung und Haftung offen.

Um ein angemessenes Sicherheitsniveau innerhalb einer Organisation zu erreichen, müssen die Mitarbeiter die IT-Sicherheitsaspekte ihrer Arbeit kennen und beachten.

Eine sinnvolle Vorgehensweise zur Vermittlung dieser Sicherheitsaspekte ist die zielgruppengerechte Aufbereitung des Sicherheitskonzeptes der Organisation. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) empfiehlt daher, die einzelnen Sicherheitsthemen bedarfsgerecht in unterschiedlichen Sicherheitsrichtlinien und Teilkonzepten darzustellen. So erhalten Mitarbeiter genau die Informationen, die sie benötigen.

Informationssicherheit besteht darin, die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen sicherzustellen. Gleichzeitig wird das Risiko des Verlusts oder der unerlaubten Offenlegung solcher Informationen durch die Implementierung von Richtlinien, von standardisierten Prozessen und Verfahren durch geeignete Sicherheitsmaßnahmen minimiert.

## INHALTE EINER IT-SECURITY RICHTLINIE

- Antivirus
- Clear Desk
- Datenschutz
- E-Mail Nutzung
- Internet Nutzung
- IT-Equipment
- Backup & Restore
- Mobile Datenverarbeitung
- Passwörter
- Software Nutzung
- Verschlüsselung
- Zugriffskontrolle
- Heimarbeit
- Physikalische Sicherheit
- Verantwortlichkeiten
- Datenklassifizierung
- Security Awareness
- Patch Management

## ZIELE EINER IT-SECURITY RICHTLINIE

### SIE MÖCHTEN SICHERSTELLEN, DASS

- Informationen vor unbefugtem Zugriff oder Missbrauch geschützt werden,
- die Vertraulichkeit von Informationen gewährleistet ist,
- die Integrität von Informationen gewahrt bleibt,
- die wesentlichen Unternehmensprozesse auch in Notfallsituationen aufrechterhalten werden (Business Continuity),
- gegebenenfalls IT-Standards und IT-Richtlinien entwickelt und Maßnahmen zu deren Unterstützung implementiert werden,
- alle relevanten Datenschutzbestimmungen (auf europäischer und nationaler Ebene) eingehalten werden,
- eine hohe, jederzeit den Businessanforderungen gerecht werdende Verfügbarkeit der informationsverarbeitenden Systeme und Services aufrechterhalten wird,
- gewährleistet ist, dass kein Abfluss streng vertraulicher Informationen an Unbefugte erfolgen kann mit der zu erwartenden Folge einer Schädigung Ihrer Marke.

## Kontakt

Sie haben Fragen zum Thema?

Wenden Sie sich bitte an

**Daniel Leiendecker**

Business Development Manager | ectacom GmbH

**Email:** [dleiendecker@ectacom.com](mailto:dleiendecker@ectacom.com)

