

# Managementhandbuch

## Kapitel 1.7 Informationssicherheitsrichtlinie

---

Wir sehen es als Grundlage unseres unternehmerischen Handelns an, unsere Betriebs- und Geschäftsgeheimnisse zu schützen. Der Schutz von durch Kunden und Partnern bereitgestellten Informationen ist uns hierbei genauso wichtig wie der Schutz des eigenen Know-how.

Die vorliegende Richtlinie ist für das gesamte Unternehmen gültig. Der Geltungsbereich des Managementsystems erstreckt sich auf Forschung und Entwicklung, Sicherheitsbewertung und Projektträgerschaften auf dem Gebiet der Anlagen- und Reaktorsicherheit, Entsorgung, Endlagerung, Stilllegung und des Umweltschutzes.

Ziel der vorliegenden Informationssicherheitsrichtlinie und der daraus abgeleiteten Richtlinien ist es, Informationen vor internen und externen Bedrohungen zu schützen, die Fortführung des Geschäftsbetriebes sicherzustellen und mögliche Schäden durch Sicherheitsvorfälle so weit wie möglich zu minimieren. Informationen können in vielfältiger Form vorliegen. Sie können elektronisch gespeicherte oder übermittelte Daten als auch Informationen auf Papier umfassen.

Als wichtigste Sicherheitsziele für die GRS sehen wir die Einhaltung der Vertraulichkeit, Integrität und Verfügbarkeit unserer Unternehmensdaten und IT-Systeme sowie der uns bereitgestellten Informationen unserer Geschäftspartner an.

Grundlage für die Auswahl von technischen und organisatorischen Maßnahmen sind die Einhaltung gesetzlicher, regulatorischer und vertraglicher Verpflichtungen und die Forderungen der ISO/IEC 27001:2013. Darüber hinaus dienen die Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als Orientierung. Die GRS ist bestrebt, die Eignung, Angemessenheit und Wirksamkeit ihrer Maßnahmen zur Informationssicherheit fortlaufend zu verbessern.

Der IT-Sicherheitsbeauftragte und der Compliance Officer erstellen die Richtlinien im Bereich der Informationssicherheit in Zusammenarbeit mit den betroffenen Organisationseinheiten, legen diese der Geschäftsführung zur Freigabe vor, stellen die Kommunikation an die betroffenen Personenkreise sicher und überwachen deren Umsetzung. Der IT-Sicherheitsbeauftragte und der Compliance Officer sind direkt der Unternehmensleitung unterstellt und berichten an diese.

Die Bereichs- und Abteilungsleiter sind in ihren Organisationseinheiten verantwortlich für die Einführung, Einhaltung und Überwachung der Informationssicherheitsrichtlinie und der daraus abgeleiteten Richtlinien. Jeder Mitarbeiter ist verantwortlich für die Einhaltung der ihn betreffenden Regelungen der Informationssicherheitsrichtlinie und der daraus abgeleiteten Richtlinien.

### Geschäftsführung der Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Köln / Garching, den 20. Januar 2020

Hans J. Steinhauer  
Geschäftsführer

Uwe Stoll  
Geschäftsführer