Führungsaufgabe Informationssicherheit
- Das sollten Sie regeln -

RUHR UNIVERSITÄT BOCHUM

RUB

Stabsstelle für Informationssicherheit

Sichere IT-Dienste reichen nicht aus gegen

- neuartige Angriffe/Schwachstellen
- organisatorische Schwachstellen
- menschliches Fehlverhalten

Das können Sie tun:

→ Risiken erkennen und kommunizieren
→ Awareness im Team ermöglichen
→ Kommunikation und Kultur
→ Vorbild sein

Beschäftigte müssen

- über ihre Zuständigkeiten/Tätigkeiten klar und nachweisbar informiert werden.
- über daraus entstehende Risiken und deren Vermeidung informiert sein.
- mit den erforderlichen Ressourcen, Berechtigungen und Kenntnissen ausgestattet sein, die sie für ihre Tätigkeiten benötigen.
- kompetente IT-Betreuung und Ansprechpartner haben.
- über Team-/RUB-internen Umgang mit Hard-/Software und IT-Diensten informiert sein.
- über Kommunikationsregelungen informiert sein.
- für sie relevante gesetzliche und RUB-interne Regelungen kennen.
- Freiraum für Awareness- und tätigkeitsrelevante Security-Schulungen erhalten.

Personal-Dezernat

IT.SERVICES

Beschaffung

Regelwerk zur IS

(Unterstützung durch Vorlagen, Regelungen, Organisation und Technik)

Meldung von Informationssicherheitsvorfällen

1. **Wer muss melden?** Alle Beschäftigten, die einen Verdacht auf einen Vorfall haben.
2. **Wer ist einzubeziehen?** Vorgesetzte Personen/Verantwortliche; zuständige IT.
3. **Was sind typische Vorfälle?** Infektion mit Schadcode, Passwort-Kompromittierung, Datenpannen, Verlust/Diebstahl von Systemen, unbefugte Offenlegung von Daten, unbefugter Zugriff, Schwachstellen
4. **An wen wird gemeldet?** RUB-Cert / Datenschutz / Informationssicherheit

Sicherheitsvorfall
RUB-Cert
cert@rub.de

Datenpanne
DSB oder ISB
datenpanne@rub.de

Phishing
ISB oder SC
abuse@rub.de