

VERHALTEN BEI EINEM SICHERHEITSVORFALL



Ein Sicherheitsvorfall (Security Incident) ist jedes Ereignis, das die **Vertraulichkeit, Integrität oder Verfügbarkeit** von Informationen oder Systemen beeinträchtigt oder bedroht.

1

Melden

- sofortige Meldung an Informationssicherheitsbeauftragte und/oder die IT-Abteilung

2

Eindämmen

- Systeme isolieren und Zugänge sperren (sofern von IT vorgegeben)
- auf weitere Anweisungen warten

3

Analysieren

- Ursachenforschung, Schadensausmaß aus der eigenen Beobachtungsposition bestimmen und dokumentieren

4

Beobachten & dokumentieren

- Beobachtungen notieren: was, wann, wo, wer, wie, welche Auswirkungen
- Auffälligkeiten wie Fehlermeldungen, Pop-Ups oder ungewöhnliches Systemverhalten notieren

5

Keine Eigeninitiative ergreifen

- keine Anhänge öffnen, Links anklicken oder Passwörter mehrfach eingeben
- nicht versuchen, den Vorfall "selbst zu beheben"

6

Kommunikation beachten

- keine Informationen über den Vorfall nach außen geben (z. B. Teammitglieder oder Externe)
- nur offizielle Kommunikationswege nutzen

7

Gerät sichern

- Betroffenes Gerät nicht mehr für weitere Arbeit nutzen, bis Rückmeldung der IT erfolgt ist