05_Notfall- & Kontinuitätsmanagement (BSI 200-4 Light)

- Notfallhandbuch
  - Notfallkarte – Vorlage
  - Kontaktliste
  - IT-Fibel Notfallplan SPIEGELBLANK
- Business-Impact-Analyse (BIA)
  - BIA – Kernprozesse
- Wiederanlaufpläne (IR/DR)
  - Wiederanlauf – Szenarien
  - Übungen & Tests
- Kommunikations- & Eskalationsplan
  - Kommunikationsplan

Notfallhandbuch

Notfallkarte – Vorlage

Notfallkarte: {{Szenario}}

Auslöser: {{z. B. Ransomware, DC-Ausfall}}
Priorität/RTO: {{z. B. 8h}} | **RPO:** {{z. B. 4h}}

Team & Kontakte

Leitung, Technik, Kommunikation, externe Partner

Sofortmaßnahmen (0–2 h)

1. Isolieren 2) Beweise sichern 3) Kommunikationslinie aktivieren

Wiederanlauf (2–8 h)

Systemreihenfolge, Checklisten, Abnahmekriterien

Kommunikation

Meldeschwellen (Behörde/Kunden), Vorlagen, Freigabe

Nachbereitung

Root-Cause, Maßnahmenplan, Lessons Learned

Kontaktliste

Kontaktliste

Rolle	Name	Kontakt

IT-Fibel Notfallplan SPIEGELBLANK

siehe Anhänge

auch zu finden in Sharepoint IT > Cybersecurity

Business-Impact-Analyse (BIA)

BIA – Kernprozesse

BIA – Kernprozesse

Prozess	Max. Ausfallzeit (MTPD)	RTO	RPO	Minimalbetrieb	Bemerkungen
Lohnabrechnung	{{}}	{{}}	{{}}	{{}}	
Tourenplanung	{{}}	{{}}	{{}}	{{}}	

Wiederanlaufpläne (IR/DR)

Wiederanlauf – Szenarien

Wiederanlauf – Szenarien

(Systemprioritäten, Reihenfolge, technische Schritte)

Übungen & Tests

Übungen & Tests

(Planung, Durchführung, Protokolle, Verbesserungsmaßnahmen)

Kommunikations- & Eskalationsplan

Kommunikationsplan

Kommunikationsplan

(Stakeholder, Vorlagen, Freigaben)