IT-NOTFALLPLAN

Interaktives Dokument mit Ausfüllfeldern

Gemäß:

- ISO 22301:2019 - Business Continuity Management Systems
- BSI IT-Grundschutz (DER.4 Notfallmanagement, CON.3 Datensicherungskonzept)
- NIST SP 800-34 Rev. 1 - Contingency Planning Guide
- COBIT 2019 (DSS04 Manage Continuity)

Dokumenteninformationen

Unternehmensname	
Abteilung	
Dokumentennummer	
Version	
Erstellt am	
Nächster Review	
Verantwortlich	
Freigegeben von	

Inhaltsverzeichnis

1. Verantwortlichkeiten und Organisation

1.1 Krisenstab

Vorsitz (Name):

Funktion:

Stellvertreter:

Telefon (Dienst):

Telefon (Privat):

1.2 IT-Notfallbeauftragter

Name:

Abteilung:

Telefon (Dienst):

Telefon (Privat):

E-Mail:

1.3 Eskalationsmatrix

Stufe	Situation	Verantwortlich	Maßnahme	Zeitrahmen
1	Einzelner Systemausfall	IT-Betrieb	Lokale Wiederherstellung	< 1 Stunde
2	Mehrere Systeme	IT-NB	Koordination Recovery	< 4 Stunden
3	Gesamtunternehmen	Krisenstab	Vollständiger Notfallmodus	< 1 Tag
4	Cyber-Angriff	CISO + Krisenstab	Isolation + Forensik	Sofort

Notizen zur Eskalationsmatrix:

2. Business Impact Analysis (BIA)

2.1 Kritische Geschäftsprozesse

Beschreiben Sie die kritischsten Geschäftsprozesse und deren Abhängigkeiten:

2.2 RTO/RPO-Definitionen

RTO = Recovery Time Objective (Max. Ausfallzeit) | RPO = Recovery Point Objective (Max. Datenverlust)

System/Prozess	RTO	RPO	Priorität	Verantwortlich

2.3 Finanzielle Auswirkungen

Kosten pro Stunde Ausfall für kritische Systeme:

System	Kosten/Stunde	Tageskosten	Wochenkosten
_____ EUR	_____ EUR	_____ EUR	_____ EUR
_____ EUR	_____ EUR	_____ EUR	_____ EUR
_____ EUR	_____ EUR	_____ EUR	_____ EUR
_____ EUR	_____ EUR	_____ EUR	_____ EUR

2.4 Abhängigkeiten und Schnittstellen

3. Risikobewertung

3.1 Bedrohungsszenarien

Bedrohung	Wahrsch.	Schaden	Risiko	Maßnahme
Ransomware	H/M/N	H/M/N	___	_____
Cloud-Ausfall	H/M/N	H/M/N	___	_____
Hardware-Ausfall	H/M/N	H/M/N	___	_____
Brand/Wasser	H/M/N	H/M/N	___	_____
Cyber-Angriff	H/M/N	H/M/N	___	_____
Lieferantenausfall	H/M/N	H/M/N	___	_____
Personalnot	H/M/N	H/M/N	___	_____
Stromausfall	H/M/N	H/M/N	___	_____

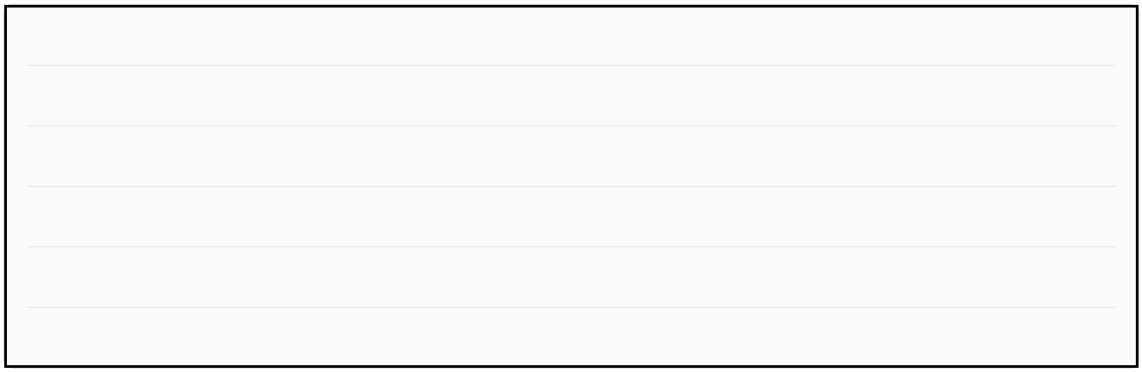
3.2 Bestehende Schutzmaßnahmen

3.3 Risikobewertungsmatrix

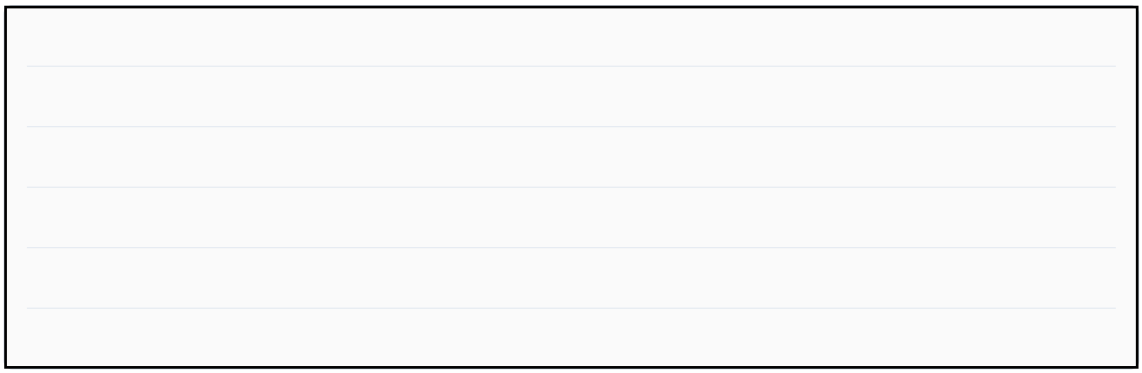
	Geringer Schaden	Mittlerer Schaden	Hoher Schaden
Sehr wahrscheinlich	MITTEL	HOCH	KRITISCH
Wahrscheinlich	NIEDRIG	MITTEL	HOCH
Möglich	NIEDRIG	NIEDRIG	MITTEL
Unwahrscheinlich	NIEDRIG	NIEDRIG	NIEDRIG

4. Wiederherstellungsstrategien

4.1 Backup-Strategie



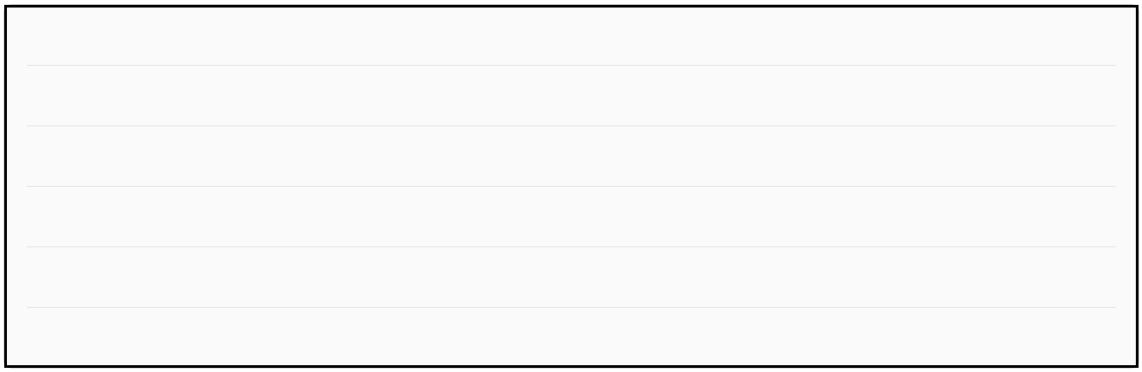
4.2 Replikationsstrategie



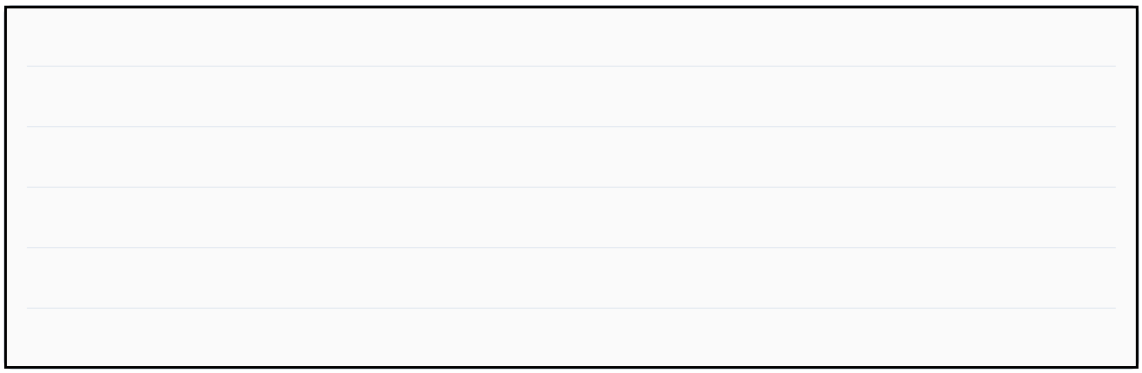
4.3 Cloud-DR-Strategie

4. Wiederherstellungsstrategien (fortg.)

4.4 Organisatorische Strategien



4.5 Personelle Strategien

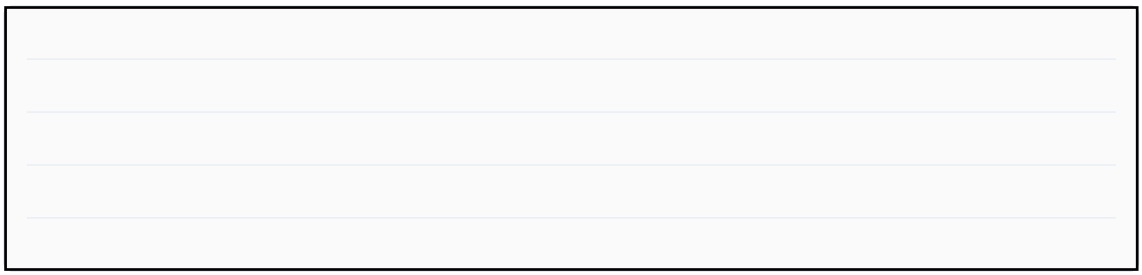


4.6 Ransomware-spezifische Recovery

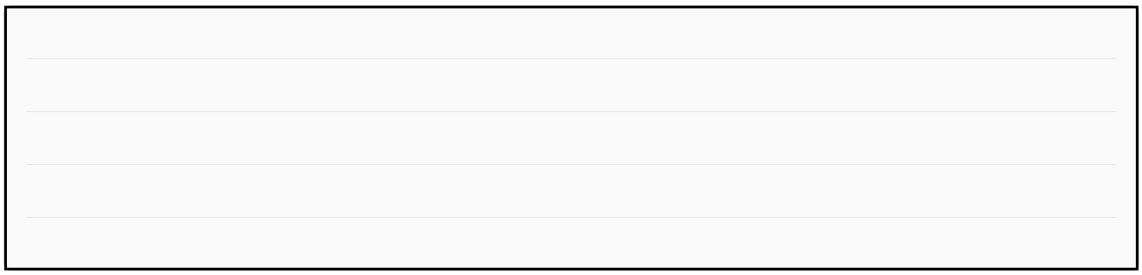
5. Detaillierte Wiederherstellungspläne

5.1 System 1: _____

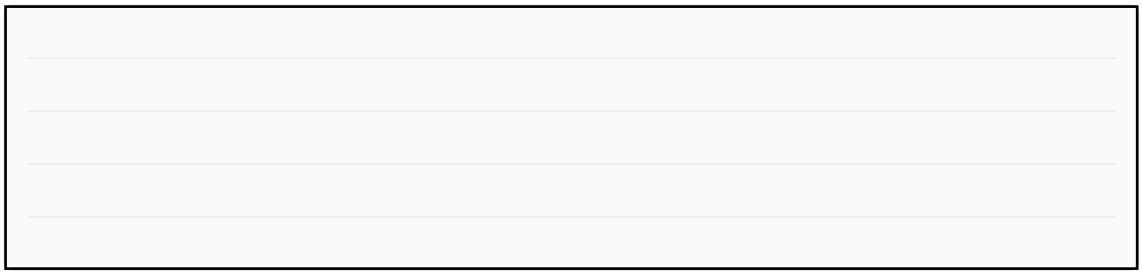
Schritt 1: Sofortmaßnahmen (erste 15 Minuten)



Schritt 2: Bewertung (15-60 Minuten)



Schritt 3: Wiederherstellung (ab 60 Minuten)



Schritt 4: Verifikation

5. Detaillierte Wiederherstellungspläne (fortg.)

5.2 System 2: _____

Schritt 1: Sofortmaßnahmen

Schritt 2: Bewertung

Schritt 3: Wiederherstellung

Schritt 4: Verifikation

6. Kommunikationsplan

6.1 Interne Kommunikation

Wer wird wann informiert?

6.2 Externe Kommunikation

Kunden, Lieferanten, Behörden:

6.3 Medienkommunikation

Presse, Öffentlichkeit:

6. Kommunikationsplan (fortg.)

6.4 Meldepflichten

DSGVO (72 Stunden), KRITIS, NIS-2:

6.5 Kommunikationskanäle im Notfall

Wenn das normale Netzwerk nicht verfügbar ist:

7. Test- und Übungsplan

7.1 Testarten und Frequenz

Testart	Frequenz	Umfang	Verantwortlich	Nächster Termin
Tabletop-Übung	Quartalsweise	Gesamtorganisation	_____	_____
Funktionstest	Halbjährlich	Einzelne Systeme	_____	_____
Volltest	Jährlich	Alle Systeme	_____	_____
Cyber-Simulation	Jährlich	IT-Abteilung	_____	_____

7.2 Testprotokoll

Datum des letzten Tests:

Teilnehmer:

Ergebnisse:

8. Compliance-Checkliste

8.1 ISO 22301

- [ ] Business Impact Analysis durchgeführt
- [ ] Risikobewertung aktuell
- [ ] Wiederherstellungspläne dokumentiert
- [ ] Tests regelmäßig durchgeführt
- [ ] Management-Commitment vorhanden
- [ ] Kontinuierliche Verbesserung nachweisbar

8.2 BSI IT-Grundschutz

- [ ] DER.4 Notfallmanagement umgesetzt
- [ ] CON.3 Datensicherungskonzept vorhanden
- [ ] Bedrohungsanalyse aktuell
- [ ] Schutzmaßnahmen implementiert
- [ ] Regelmäßige Überprüfung

8.3 NIST SP 800-34

- [ ] CP-1: Contingency Planning Policy vorhanden
- [ ] CP-2: Contingency Plan erstellt
- [ ] CP-3: Training durchgeführt
- [ ] CP-4: Tests regelmäßig
- [ ] CP-9: System Backup implementiert
- [ ] CP-10: Recovery procedures dokumentiert

8.4 COBIT DSS04

- [ ] BIA durchgeführt
- [ ] Business Continuity Pläne dokumentiert
- [ ] Pläne regelmäßig getestet
- [ ] Backup- und Recovery-Verfahren implementiert

9. Quick-Reference-Cards

9.1 Card 1: Sofortmaßnahmen bei IT-Ausfall

1	Notfall hotline anrufen: _____	☐
2	Systemstatus prüfen	☐
3	Krisenstab informieren	☐
4	Schadensbegrenzung einleiten	☐
5	Dokumentation beginnen	☐

9.2 Card 2: Ransomware-Angriff

1	Betroffene Systeme SOFORT isolieren	☐
2	Netzwerkverbindung trennen	☐
3	CISO/IT-Leitung informieren	☐
4	Keine Daten löschen oder bezahlen!	☐
5	Forensisches Team einschalten	☐
6	Backup-Integrität prüfen	☐
7	Behörden informieren (BKA/LKA)	☐

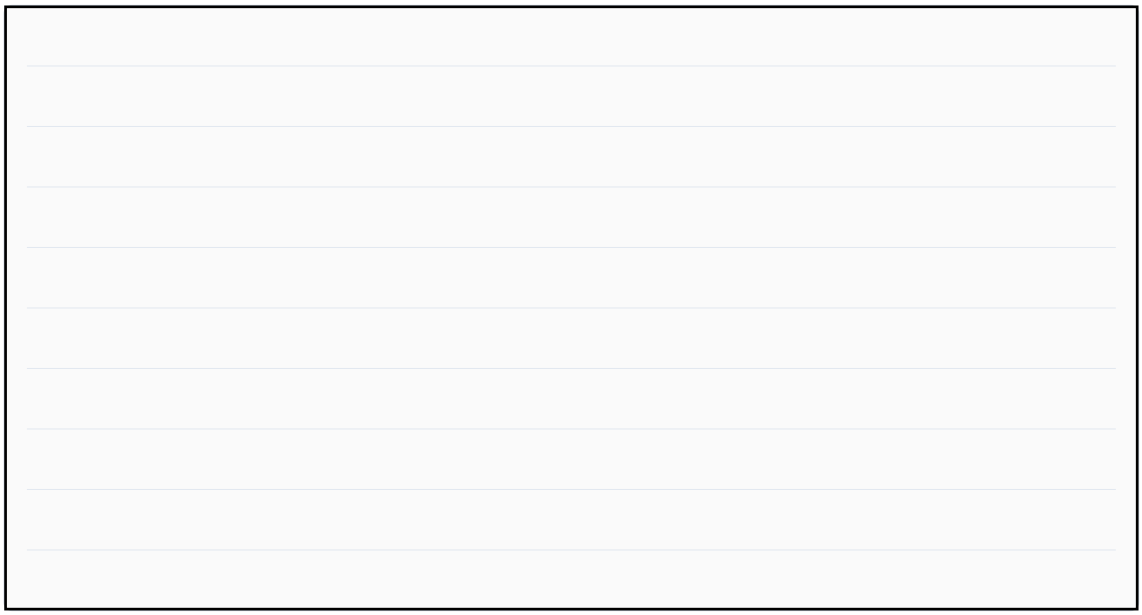
9.3 Notfall-Kontaktliste

Rolle	Name	Tel (Dienst)	Tel (Privat)	E-Mail
Krisenstab Vorsitz				
IT-Notfallbeauftragter				
CISO				
Geschäftsführung				
Externer IT-Dienstleister				
Versicherung				
Behörden				

10. Anhänge und Notizen

10.1 Systemlandkarte

Zeichnen Sie hier die wichtigsten Systemabhängigkeiten ein:



10.2 Vendor-Kontaktliste

Hersteller	Produkt/Service	Support-Tel	Vertragsnr.

10.3 Freigabeprotokoll

Version	Datum	Geändert von	Freigegeben	Änderungen

10.4 Allgemeine Notizen