VORLAGE · BUSINESS CONTINUITY

IT-Notfallplan

Anpassbare Vorlage, orientiert am BSI-Standard 200-4. Ersetzen Sie die *kursiv/grau* markierten Platzhalter durch Ihre Organisationsdaten. Halten Sie ein aktuelles Exemplar ausgedruckt und offline bereit – im Ernstfall sind Fileserver, Wiki und E-Mail oft nicht erreichbar. Stand: 09/2026.

Organisation	_____	Dokument-Version	1.0
Verantwortlich (IT-Notfallkoordination)	_____	Klassifizierung	Vertraulich
Gültig ab	__ / __ / ____	Nächste Überprüfung	__ / __ / ____
Freigegeben durch	_____	Ablage offline / Papier	_____

1. Zweck & Geltungsbereich

Dieser Plan legt fest, wie *[Organisation]* bei einem schweren Ausfall der IT alarmiert, entscheidet, Sofortmaßnahmen ergreift und die kritischen IT-Services in der festgelegten Reihenfolge wieder in Betrieb nimmt. Er ist Teil des Notfallhandbuchs und ergänzt den Incident-Response-Plan.

Festlegung	Inhalt
Standorte	*z. B. Hauptsitz, Rechenzentrum, Außenstellen*
IT-Services / Systeme im Geltungsbereich	*siehe Abschnitt 6*
Nicht im Geltungsbereich	*z. B. Produktions-OT (eigener Plan)*
Aktivierung des Plans durch	*Rolle / Name, Vertretung*
Aktivierungskriterien	*z. B. Eskalationsstufe „Notfall“ (Abschnitt 4)*
Deaktivierung / Rückkehr in den Normalbetrieb durch	*Rolle / Name*

2. Alarmierungs- & Kontaktliste

Interne Kontakte

Funktion	Name	Mobil (dienstl. / privat)	Vertretung	Erreichbar
Leitung Notfallstab	*Name*	*Tel*	*Name / Tel*	*24/7*
IT-Notfallkoordination	*Name*	*Tel*	*Name / Tel*	*24/7*
Informationssicherheit (ISB / CISO)	*Name*	*Tel*	*Name / Tel*	…
Geschäftsleitung	*Name*	*Tel*	*Name / Tel*	…
Kommunikation	*Name*	*Tel*	*Name / Tel*	…
Datenschutz / Recht	*Name*	*Tel*	*Name / Tel*	…
…	…	…	…	…

Externe Kontakte

Partner	Ansprechpartner	Telefon (Notfall)	Vertrags- / Kundennummer
IT-Dienstleister / Systemhaus	*Name*	*Tel*	*Nr.*
Rechenzentrum / Cloud-Anbieter	*Name*	*Tel*	*Nr.*
Internet- / Telefonie-Provider	*Name*	*Tel*	*Nr.*
Forensik- / Incident-Response-Dienstleister	*Name*	*Tel*	*Nr.*
Cyberversicherung	*Schadenhotline*	*Tel*	*Police-Nr.*
Meldestelle NIS2 (DE: BSI · AT: CSIRT)	—	*Tel / Portal*	*Registrierungs-Nr.*
Datenschutzaufsicht	*zust. Behörde*	*Tel / Portal*	—
Polizei / Strafverfolgung	*Cybercrime-Stelle*	*Tel*	—

3. Rollen (Notfallstab / BAO)

Die Besondere Aufbauorganisation (BAO) wird mit Aktivierung des Plans eingesetzt und bleibt bis zur Deaktivierung zuständig.

Rolle	Aufgabe	Befugnisse	Name	Vertretung
Leitung Notfallstab	Gesamtsteuerung, Priorisierung, Entscheidungen	*z. B. Notfallbudget bis … €*	*Name*	*Name*
IT-Notfallkoordination	Lage IT, Wiederanlauf nach Abschnitt 6	*z. B. Abschaltung von Systemen*	*Name*	*Name*
Informationssicherheit	Sicherheitsbewertung, Beweissicherung, Schnittstelle IR-Team	*z. B. Isolation von Netzsegmenten*	*Name*	*Name*
Kommunikation	Interne und externe Kommunikation	*Freigabe nach Abstimmung mit Leitung*	*Name*	*Name*
Recht / Datenschutz	Meldepflichten, Verträge, Datenschutz	…	*Name*	*Name*
Protokoll / Lage	Ereignisprotokoll (Abschnitt 9), Lagebild	…	*Name*	*Name*
Fachbereichsvertretung	Auswirkungen auf Geschäftsprozesse, Notbetrieb	…	*Name*	*Name*

4. Eskalationsstufen (Störung / Notfall / Krise)

Stufe	Merkmale (Beispiele – anpassen)	Bewältigung durch	Entscheidung über Stufe
Störung	Einzelne Systeme oder Nutzer betroffen, Behebung im Regelbetrieb innerhalb der vereinbarten Zeiten möglich	IT-Betrieb / Service Desk	*Rolle*
Notfall	Kritische IT-Services fallen aus, RTO aus Abschnitt 6 ist gefährdet, Geschäftsbetrieb stark beeinträchtigt	Notfallstab (BAO), dieser Plan	*Rolle*
Krise	Lage ist mit den vorbereiteten Plänen nicht mehr zu bewältigen, z. B. Ausfall mehrerer Standorte, großflächiger Cyberangriff, öffentliche Wirkung	Krisenstab unter Leitung der Geschäftsleitung	*Rolle*

5. Sofortmaßnahmen-Checkliste

Erste 15 Minuten

- [ ] Meldung aufnehmen: Zeitpunkt, Melder, betroffene Systeme, Symptome – Protokoll starten (Abschnitt 9)
- [ ] Eskalationsstufe festlegen (Abschnitt 4) und Plan aktivieren
- [ ] IT-Notfallkoordination und Leitung Notfallstab alarmieren (Abschnitt 2)
- [ ] Bei Verdacht auf Cyberangriff: Isolationsentscheidung treffen, Informationssicherheit einbinden

Erste 60 Minuten

- [ ] Notfallstab einberufen – bei kompromittierter Infrastruktur über den Ersatzkanal (Abschnitt 8)
- [ ] Lagebild erstellen: Umfang, betroffene IT-Services, Auswirkungen auf Geschäftsprozesse
- [ ] Schaden begrenzen: betroffene Systeme trennen, Zugänge sperren, keine Systeme vorschnell neu aufsetzen
- [ ] Beweise sichern (Logs, Images) vor Bereinigung oder Wiederherstellung

- [ ] Meldepflichten prüfen und Fristbeginn dokumentieren (Abschnitt 8)
- [ ] Backups auf Verfügbarkeit und Integrität prüfen, Wiederanlauf nach Abschnitt 6 planen
- [ ] Erste interne Information an Mitarbeitende: was tun, was nicht tun

6. Kritische IT-Services: RTO/RPO & Wiederanlauf-Reihenfolge

Werte aus der Business Impact Analyse übernehmen. Die Priorität bestimmt die Reihenfolge des Wiederanlaufs; Abhängigkeiten beachten (ein Dienst kann erst starten, wenn seine Voraussetzungen laufen).

Prio	IT-Service	Gestützte Prozesse	Abhängig von	RTO	RPO	Verantwortlich	WAP-Nr.
1	*z. B. Netzwerk / Firewall*	*alle*	*Strom, Provider*	*h*	*h*	*Name*	*WAP-01*
1	*z. B. Identitätsdienst (Verzeichnisdienst)*	*alle*	*Netzwerk*	*h*	*h*	*Name*	*WAP-02*
1	*z. B. Backup-Infrastruktur*	*Wiederherstellung*	*Netzwerk, Identität*	*h*	*—*	*Name*	*WAP-03*
2	*z. B. ERP*	*Auftrag, Rechnung*	*Datenbank*	*h*	*h*	*Name*	*WAP-04*
2	*z. B. E-Mail / Kollaboration*	*Kommunikation*	*Identität*	*h*	*h*	*Name*	*WAP-05*
…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…

RTO = Recovery Time Objective (Zielzeit bis zum Wiederanlauf) · RPO = Recovery Point Objective (maximal tolerierbarer Datenverlust als Zeitraum vor der Störung).

7. Verweise auf Wiederanlaufpläne

Die technischen Einzelschritte je System stehen in eigenen Wiederanlaufplänen (WAP). Jeder WAP muss auch offline verfügbar sein.

WAP-Nr.	System / Service	Ablage online	Ablage offline / Papier	Letzter Test	Verantwortlich
WAP-01	…	*Pfad*	*Ort*	*__ / __ / ____*	*Name*
WAP-02	…	*Pfad*	*Ort*	*__ / __ / ____*	*Name*
WAP-03	…	*Pfad*	*Ort*	*__ / __ / ____*	*Name*
…	…	…	…	…	…

8. Kommunikation (intern / extern / Behörden)

Zielgruppe	Verantwortlich	Kanal (primär)	Ersatzkanal (out-of-band)	Freigabe durch
Notfallstab	Leitung Notfallstab	*z. B. Telefonkonferenz*	*z. B. vorab vereinbarter externer Messenger*	—
Mitarbeitende	Kommunikation	*Intranet / E-Mail*	*SMS-Verteiler, Aushang*	*Rolle*
Kunden / Partner	Kommunikation + Leitung	*E-Mail / Statusseite*	*Telefon*	*Rolle*
Dienstleister	IT-Notfallkoordination	*Hotline*	…	—
Öffentlichkeit / Presse	Kommunikation	*Statement*	…	*Geschäftsleitung*

Behörden und Meldepflichten

Empfänger	Wann	Frist ab Kenntnisnahme	Zuständig
NIS2-Meldestelle (DE: § 32 BSIG · AT: § 34 NISG 2026)	erheblicher Sicherheitsvorfall	Frühwarnung 24 h · Meldung 72 h · Abschlussbericht 1 Monat nach der Meldung	*Rolle*
Datenschutzaufsicht (Art. 33 DSGVO)	Verletzung des Schutzes personenbezogener Daten	unverzüglich, möglichst binnen 72 h	*Rolle*
Weitere (z. B. Branchenaufsicht, Versicherung, Polizei)	…	…	*Rolle*

Fristen als Orientierung – im Einzelfall die geltenden Gesetzestexte (NIS2-Richtlinie Art. 23, BSIG, NISG 2026, DSGVO) und Behörden-Vorgaben prüfen.

9. Dokumentation / Ereignisprotokoll

Alle Informationen, Entscheidungen und Maßnahmen mit Uhrzeit festhalten – auf Papier, falls IT-Systeme nicht verfügbar sind. Das Protokoll ist Grundlage für Meldungen, Versicherung, Nachbereitung und Audit.

Datum / Uhrzeit	Ereignis / Information	Entscheidung / Maßnahme	Wer
__.__. __:__	…	…	*Name*
__.__. __:__	…	…	*Name*
__.__. __:__	…	…	*Name*
__.__. __:__	…	…	*Name*
__.__. __:__	…	…	*Name*

Nach Abschluss: Nachbereitung (After-Action-Review) mit Maßnahmen, Verantwortlichen und Fristen; Plan, Kontaktliste und Wiederanlaufpläne aktualisieren.

10. Test- & Übungsplan

Ein ungetesteter Plan ist eine Annahme. Planen Sie die drei Stufen mit Termin und Verantwortlichem und halten Sie Ergebnisse und Maßnahmen fest.

Übungsart	Inhalt / Szenario	Geplant am	Verantwortlich	Durchgeführt am	Ergebnis / Maßnahmen
Planbesprechung	*Plan gemeinsam durchgehen: vollständig, korrekt, aktuell?*	__ / __ / ____	*Name*	__ / __ / ____	…
Tabletop-Übung	*z. B. Ransomware-Szenario mit Notfallstab*	__ / __ / ____	*Name*	__ / __ / ____	…
Funktionstest	*z. B. Restore-Test WAP-03, Wiederanlauf ERP*	__ / __ / ____	*Name*	__ / __ / ____	…
…	…	…	…	…	…

Beispiel-Häufigkeiten nach BSI-Standard 200-4: Planbesprechung zeitnah nach Erstellung und nach wesentlichen Änderungen · Funktionstest mindestens jährlich bei RTO unter 24 h, mindestens alle 3 Jahre bei RTO unter 5 Tagen · Stabsübung mindestens jährlich.

11. Freigabe

Schritt	Name / Funktion	Datum	Unterschrift
Erstellt	*Name, Funktion*	__ / __ / ____	
Geprüft	*Name, Funktion*	__ / __ / ____	
Freigegeben (Geschäftsleitung)	*Name, Funktion*	__ / __ / ____	

Änderungshistorie

Version	Datum	Änderung	Autor
1.0	__ / __ / ____	Ersterstellung aus Vorlage	*Name*
…	…	…	…

> **Diese Vorlage ist ein Ausgangspunkt, kein fertiger Plan.** Ein IT-Notfallplan wirkt erst, wenn er auf Ihre Organisation zugeschnitten *und* geübt ist. Testen Sie ihn in einer Tabletop-Übung, bevor es zählt: secdrills.com/check.