rimerit



VORLAGE ZUM AUSFÜLLEN · IT-SICHERHEIT

IT-Notfallplan für Unternehmen

Was im Ernstfall zu tun ist, wer entscheidet und welche Systeme zuerst wieder laufen müssen.

DIESER PLAN GEHÖRT ZU

Unternehmen

Standort

Verantwortlich für diesen Plan

Version / Stand vom

Im Notfall: die ersten Minuten

Diese Seite gut sichtbar aushängen. Sie gilt für alle Mitarbeitenden.

1. **Ruhe bewahren.** Nichts überstürzt löschen, neu installieren oder „ausprobieren“.
2. **Notfall sofort melden.** An die Notfall-Rufnummer unten. Lieber einmal zu viel melden als zu spät.
3. **Bei Verdacht auf Angriff: Gerät vom Netz trennen.** Netzwerkkabel ziehen, WLAN ausschalten. Nicht einfach herunterfahren, außer die IT sagt es.
4. **Beobachtungen notieren.** Was ist passiert? Wann? An welchem Gerät? Fehlermeldung fotografieren.
5. **Keine Lösegeldforderung beantworten** und keine Links oder Anhänge mehr öffnen.
6. **Anweisungen der Notfallverantwortlichen folgen.** Informationen nach außen gibt nur, wer dafür benannt ist.

Notfall-Rufnummer

Name / Funktion	Telefon (mobil)
Vertretung	Telefon (mobil)

Diese Angaben bei der Meldung durchgeben

Wer meldet?	
Welches Gerät oder System ist betroffen?	
Was ist aufgefallen?	
Wann ist es aufgefallen?	
Wo steht das Gerät?	

Nicht jedes IT-Problem ist ein Notfall

Legen Sie vorher fest, was als Störung, Ausfall oder Sicherheitsvorfall gilt. Dann weiß jeder, wie schnell eskaliert wird.

1

Einzelne Störung

Ein Gerät oder Programm fällt aus. Der Betrieb läuft weiter.

z. B. Drucker defekt

2

Betriebs-unterbrechung

Wichtige Systeme fallen aus. Mehrere Personen können nicht arbeiten.

z. B. Server oder E-Mail weg

3

Sicherheitsvorfall

Verdacht auf Angriff, Datenabfluss oder Verschlüsselung.

z. B. Dateien unlesbar

Auf den Linien eigene Beispiele aus Ihrem Unternehmen eintragen.

Wer wird je Stufe informiert?

Stufe	Wer wird informiert?	Spätestens nach	Wer entscheidet?
Beispiel	*IT-Dienstleister, Geschäftsführung*	*30 Minuten*	*Geschäftsführung*
Stufe 1			
Stufe 2			
Stufe 3			

Kontakte und Zuständigkeiten

Jede Rolle braucht eine Vertretung. Zwei Mal im Jahr prüfen, ob die Nummern noch stimmen.

Rolle	Name	Telefon	Vertretung
Notfallverantwortliche/r			
Geschäftsführung			
IT intern			
IT-Dienstleister			
Datenschutzbeauftragte/r			
Internetanbieter			
Telefonanbieter			
Cyber-Versicherung (Schaden-Nr.)			
Wichtige Softwarehersteller			
Polizei / Cybercrime-Stelle			

Wer darf was entscheiden?

Entscheidung	Zuständig	Vertretung
Systeme abschalten oder vom Netz nehmen		
Mitarbeitende informieren		
Kunden und Partner informieren		
Externe Hilfe beauftragen		
Meldung an Behörden und Versicherung		

Kritische Systeme und Wiederanlauf

Welche Systeme müssen zuerst wieder laufen? Und wovon hängen sie ab? Ohne Netzwerk und Zugänge startet oft auch der Server nicht sinnvoll.

Prio	System	Hängt ab von	Max. Ausfall	Zuständig
1	*Netzwerk / Firewall*	*Strom, Internet*	*2 Std.*	*IT-Dienstleister*
2	*Microsoft 365*	*Internet, Konten*	*4 Std.*	*IT intern*

Typische kritische Systeme: Server, Microsoft 365, Cloud-Dienste, Warenwirtschaft oder ERP, Telefonanlage, Netzwerk und Firewall, Branchensoftware.

Notbetrieb: wie arbeiten wir weiter?

Bereich	Notlösung
Telefon / Erreichbarkeit	
Aufträge / Kasse	
Ausweich-Kanal für das Team	

Datensicherung und Wiederherstellung

Ein Backup allein ist kein Notfallkonzept. Entscheidend ist, ob und wie schnell sich die Daten wirklich zurückholen lassen.

Was wird gesichert?	Wie oft?	Wo gespeichert?	Dauer bis wieder da	Zuletzt getestet
Dateiserver	*täglich*	*NAS + Offline-Kopie*	*ca. 6 Std.*	*03/2026*

Kurz prüfen

- [ ] Mindestens eine Sicherung liegt getrennt vom Firmennetz.
- [ ] Die Wiederherstellung wurde im letzten Jahr wirklich ausprobiert.
- [ ] Es ist klar, wer die Wiederherstellung startet und freigibt.
- [ ] Die Zugänge zur Sicherung sind auch bei Serverausfall erreichbar.

Wichtig: Zugangsdaten gehören nicht in diesen Plan. Notieren Sie nur, *wo* sie sicher hinterlegt sind, zum Beispiel im Passwortmanager oder im Tresor.

Kommunikation und Protokoll

Im Ernstfall laufen E-Mail und Telefonanlage oft nicht. Legen Sie vorher fest, wer was übernimmt.

Wer informiert Kunden?	
Ablageort dieses Plans (gedruckt)	
Zugangsdaten hinterlegt bei / in	

Meldepflichten beachten: Sind personenbezogene Daten betroffen, ist ein Vorfall in der Regel innerhalb von 72 Stunden der zuständigen Datenschutz-Aufsichtsbehörde zu melden (Art. 33 DSGVO). Ziehen Sie früh Ihre Datenschutzbeauftragte bzw. Ihren Datenschutzbeauftragten hinzu. Bei einer Cyber-Versicherung gelten zusätzlich deren Meldefristen.

Notfall-Protokoll

Während des Vorfalls laufend ausfüllen. Hilft bei Versicherung, Behörden und der Auswertung danach.

Datum / Uhrzeit	Was ist passiert?	Maßnahme	Wer?

Testen und aktuell halten

Ein Plan, der nie geprobt wurde, funktioniert im Ernstfall selten. Einmal im Jahr durchspielen, nach größeren Änderungen anpassen.

- [ ] Die Verantwortlichen wissen, wo der Plan liegt.
- [ ] Alle Telefonnummern und Kontakte sind aktuell.
- [ ] Das Backup ist erreichbar und wurde wiederhergestellt.
- [ ] Die Reihenfolge der kritischen Systeme ist festgelegt.
- [ ] Neue Mitarbeitende kennen die Seite „Sofortmaßnahmen“.

Test am	Ergebnis / was angepasst wurde	Durchgeführt von

Nächster Test am

Freigegeben von (Name, Datum)

Unterstützung beim Notfallplan

TELEFON
+49 201 219609 80

E-MAIL
info@rimerit.com

WEB
rimerit.com

BÜRO
Bismarckstraße 67
45128 Essen

Haftungshinweis
Diese Vorlage dient als Orientierungshilfe. Alle Angaben erfolgen ohne Gewähr für Vollständigkeit, Richtigkeit und Aktualität. Sie ersetzt keine individuelle IT-, Datenschutz- oder Rechtsberatung. Für Entscheidungen auf Grundlage dieser Vorlage übernimmt die RIMERIT GmbH keine Haftung. Stand: Oktober 2026.