

VORLAGE · TOMORIS TOOLBOX

IT-Notfallhandbuch: Vorlage für Alarmierung, Sofortmaßnahmen und Wiederanlauf

Ausfüllbare Gliederung mit Notfallstab, Kontaktliste, Einstufung, Sofortmaßnahmen, Wiederanlauf und Übungsplan, belegt mit BSI-Standard 200-4, NIST und NISG 2026

STAND

25.10.2026

UMFANG

PDF, 10 Seiten

ONLINE

tomoris.com/downloads/it-notfallhandbuch-vorlage

AUF EINEN BLICK

3 Stufen

Störung, Notfall, Krise
nach BSI-Standard 200-4

7

Tabellen zum Ausfüllen,
von Notfallstab bis
Übungsplan

12

Monate Mindestzeitraum
der Jahresübungsplanung
(BSI)

24 h

NIS2-Frühwarnung ab
Kenntnisnahme (§ 34
NISG 2026)

FÜR WEN

- Geschäftsführung kleiner und mittlerer Unternehmen, die für den IT-Ernstfall vorsorgen will
- IT-Leitung, Informationssicherheits- und Notfallverantwortliche
- IT-Dienstleister, die mit ihren Kunden Notfallpläne erstellen und üben
- Wesentliche und wichtige Einrichtungen, die ihren Notfallplan nach NISG 2026 dokumentieren müssen

WURUM ES GEHT

Im Ernstfall fehlt die Zeit, Zuständigkeiten zu klären und Telefonnummern zu suchen. Ein IT-Notfallhandbuch bündelt vorab, was dann gebraucht wird: Rollen, Sofortmaßnahmen, Alarmierung und Eskalation sowie Kommunikations- und Wiederanlaufpläne, wie es der BSI-Baustein DER.4 beschreibt. Diese Vorlage gibt dafür eine Gliederung mit Mustertexten und Tabellen zum Ausfüllen vor. Grundlage sind der BSI-Standard 200-4, die NIST-Leitfäden SP 800-34 und SP 800-61 sowie die Anforderungen an Notfallpläne, die seit Oktober 2026 für Einrichtungen unter dem NISG 2026 gelten.

Diese Vorlage ist an Ihr Unternehmen anzupassen: Rollen, Systeme, Zielwerte und Übungsintervalle hängen von Ihren Geschäftsprozessen ab. Sie gibt einen Überblick und ersetzt keine Rechtsberatung; maßgeblich ist der Gesetzestext in der jeweils geltenden Fassung.

INHALT

01	Was ins IT-Notfallhandbuch gehört	2
02	Geltungsbereich und Notfallstab	3
03	Alarmierung und Kontaktliste	4
04	Störung, Notfall oder Krise	5
05	Sofortmaßnahmen in den ersten Minuten	6
06	Wiederanlauf: Reihenfolge und Zielwerte	7
07	Kommunikation nach innen und außen	8
08	Protokoll und Abschluss	9
09	Übungen und Pflege	9
10	Quellen	10

01 —

Was ins IT-Notfallhandbuch gehört

Inhalte nach BSI DER.4, Aufbau nach BSI-Standard 200-4 und was unter dem NISG 2026 Pflicht ist.

Das BSI beschreibt im IT-Grundschutz-Baustein DER.4 ein Notfallhandbuch mit Informationen zu Rollen, Sofortmaßnahmen, Alarmierung und Eskalation sowie Kommunikations-, Geschäftsfortführungs-, Wiederanlauf- und Wiederherstellungsplänen. Es soll Zuständigkeiten und Befugnisse festhalten, auch im Notfall zugänglich sein und regelmäßig durch Tests und Übungen geprüft werden (DER.4.A1). Für den Einstieg eignet sich nach BSI-Standard 200-4 das Reaktiv-BCMS: zuerst die Bewältigungsorganisation aufbauen und ausgewählte zeitkritische Prozesse absichern. Bestehen gesetzliche Anforderungen wie das NISG 2026, empfiehlt das BSI den Einstieg mit Aufbau- oder Standard-BCMS (Kap. 2.6.1).

Inhalte des Notfallplans für NIS2-Einrichtungen (Anhang Nr. 4.1.2 DVO (EU) 2024/2690) und wo sie in dieser Vorlage stehen

INHALT NACH NR. 4.1.2	ABSCHNITT DIESER VORLAGE
a) Zweck, Umfang und Zielgruppe; b) Rollen und Verantwortlichkeiten	02 Geltungsbereich und Notfallstab
c) wichtige Kontaktangaben, interne und externe Kommunikationskanäle	03 Alarmierung, 07 Kommunikation
d) Bedingungen für Aktivierung und Deaktivierung des Plans	04 Einstufung, 08 Protokoll und Abschluss
e) Reihenfolge der Wiederherstellung; f) Wiederherstellungspläne mit Wiederherstellungszielen; g) erforderliche Ressourcen	06 Wiederanlauf
h) Wiederaufnahme der Tätigkeiten nach vorübergehenden Maßnahmen	08 Protokoll und Abschluss

Für wesentliche und wichtige Einrichtungen ist das Pflicht: § 32 Abs. 4 lit. c NISG 2026 verlangt die Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement; seit Oktober 2026 gilt für sie der Anhang der DVO (EU) 2024/2690 samt Nr. 4.1.2, soweit angemessen (§ 2 NISV 2026). Für alle anderen Unternehmen sind die Vorgaben von BSI und NIST Empfehlungen.

02

Geltungsbereich und Notfallstab

Wofür das Handbuch gilt, wer im Stab sitzt, wer vertritt und was der Stab ohne Rückfrage entscheiden darf.

Mustertext: „Dieses Notfallhandbuch gilt für [Unternehmen] an den Standorten [Standorte] und umfasst die IT-Systeme und Dienste laut [Inventar]. Es wird angewendet, sobald ein Ereignis nach Abschnitt 04 als Notfall oder Krise eingestuft ist. Version [Nummer], freigegeben am [Datum] durch [Name, Funktion]; nächste Überprüfung am [Datum]; Ablage: [digital] und [auf Papier].“ Aufbau und Besetzung des Stabs gibt die Leitung frei (BSI-Standard 200-4, Kap. 5.1.6).

Notfallstab zum Ausfüllen: Rollen nach BSI-Standard 200-4, Kap. 5.1, je Rolle eine Vertretung (Kap. 5.1.6)

ROLLE UND AUFGABE	HAUPTZUSTÄNDIG (NAME, FUNKTION)	VERTRETUNG
Stabsleitung: koordiniert den Stab, trifft grundsätzlich die Entscheidungen	_____	_____
IT: technische Lage und Maßnahmen, Steuerung der IT-Dienstleister	_____	_____
Personal sowie Gebäude und Infrastruktur	_____	_____
Kommunikation: Informationen sammeln und für innen und außen aufbereiten	_____	_____
Protokollierung: Ereignisse und Entscheidungen festhalten	_____	_____
Nach Lage: Informationssicherheit, Datenschutz, Recht, externe Fachleute	_____	_____

Strategische Entscheidungen bleiben bei der Geschäftsführung; dem Stab sollen Entscheidungs- und Befugnisse übertragen werden (Kap. 5.1.1), etwa: [Systeme abschalten, Dienstleister beauftragen, Ausgaben bis Betrag]. Eine Person kann mehrere Rollen übernehmen (Kap. 5.1.4); bei Externen im Stab Vertraulichkeit und Befugnisse regeln (Kap. 5.1.3).

03

Alarmierung und Kontaktliste

Vom ersten Hinweis bis zum alarmierten Stab, mit Kontaktlisten intern und extern zum Ausfüllen.

1 Erkennen und melden

An die Meldestelle, z. B. IT-Hotline [Nummer]: Zeitpunkt und Ort, meldende Person, Betroffene, mögliche Ursache, ergriffene Sofortmaßnahmen, Auswirkungen, Tatsachen getrennt von Vermutungen (BSI-Standard 200-4, Kap. 5.2.1).

2 Ersteinschätzung

Die Meldestelle prüft mit einfachen Ja-Nein-Fragen (Abschnitt 04), ob ein Notfall droht. Im Zweifel gilt: lieber zu viel melden als zu wenig (Kap. 5.2.1).

3 Entscheidung

Eine zentrale, geschulte und befugte Entscheidungsinstanz, oft die Stabsleitung, stuft ein und dokumentiert Begründung und Beteiligte; der Stab bestätigt oder stuft zurück (Kap. 5.2.2).

4 Stab alarmieren

Kurz und präzise, mit Treffpunkt wie Stabsraum oder Telefonkonferenz; geregelt ist, wer wen über welche Kanäle alarmiert, auch außerhalb der Geschäftszeiten (Kap. 5.2.3).

Nicht nur per E-Mail alarmieren: Bei asynchronen Kanälen ist unklar, ob und wann die Nachricht ankommt; besser sind Anrufe auf Mobiltelefone oder Alarm-Apps (Kap. 5.2.1). Die Benachrichtigungswege während und außerhalb der Geschäftszeiten gehören dokumentiert (NIST SP 800-34, Abschnitt 4.2.2). Halten Sie Kanäle bereit, die ohne die eigene IT funktionieren (Kap. 5.2).

Kontaktliste intern: je Person mindestens eine dienstliche und eine private Nummer (NIST SP 800-34, Vorlage in Anhang A.1)

ROLLE	NAME	TELEFON DIENSTLICH	TELEFON PRIVAT
Stabsleitung	_____	_____	_____
Vertretung Stabsleitung	_____	_____	_____
IT-Verantwortung	_____	_____	_____
Kommunikation	_____	_____	_____

Datenschutz

Kontaktliste extern: mit Vertragsnummer und vertraglicher Reaktionszeit (NIST SP 800-34, Vorlage in Anhang A.1)

STELLE	ANSPRECHPERSON, TELEFON	VERTRAGS- ODER KUNDENNUMMER	REAKTIONSZEIT LAUT VERTRAG
IT-Dienstleister	_____	_____	_____
Internet, Telefonie, Cloud, Fachanwendung	_____	_____	_____
Versicherung	_____	_____	_____
CSIRT (Meldung nach NISG 2026)	_____	entfällt	entfällt
Datenschutzbehörde	_____	entfällt	entfällt
Polizei (Anzeige)	_____	entfällt	entfällt

04

Störung, Notfall oder Krise

Die drei Stufen nach BSI-Standard 200-4, Leitfragen für die Ersteinschätzung und der Bezug zur NIS2-Meldepflicht.

Stufen nach BSI-Standard 200-4, Kap. 2.1

STUFE	MERKMAL	BEWÄLTIGUNG
Störung	Prozesse oder Ressourcen stehen nicht wie vorgesehen zur Verfügung; kann zum Notfall eskalieren, wenn sie nicht in angemessener Zeit behoben wird	normale Organisation, etwa Incident-Management
Notfall	mindestens ein zeitkritischer Geschäftsprozess ist unterbrochen und im Normalbetrieb nicht innerhalb der maximal tolerierbaren Ausfallzeit wiederherstellbar; darf schon ausgerufen werden, wenn die Unterbrechung droht	Notfallstab mit vorhandenen oder anpassbaren Plänen
Krise	Schadensereignis mit erheblichen negativen Auswirkungen, für das keine passenden Notfallpläne vorliegen oder diese nicht greifen	Notfallstab, situativ

Im Ereignis sind damit zwei Fragen zu klären: Ist ein zeitkritischer Geschäftsprozess betroffen, und gibt es einen anwendbaren Plan? Leitfragen für die Meldestelle IT nach einem Beispiel des BSI (Kap. 5.2.1, Tabelle 10), anzupassen an Ihre Prozesse und so formuliert, dass sie auch ohne tiefe Fachkenntnis anwendbar sind. Mustertext: „Sobald eine Frage mit Ja beantwortet ist, sofort die Stabsleitung verständigen: [Name], Telefon [Nummer].“

- ☐ Gehört das betroffene System zur Sicherheitsinfrastruktur, etwa Virenschutz oder Firewall?
- ☐ Betrifft der Ausfall viele Benutzende oder den wesentlichen Geschäftsbetrieb?

- ☐ Besteht dringender Verdacht auf Manipulation von Daten oder Systemen, Datenabfluss, unerlaubte Ausübung von Rechten oder einen gezielten Angriff?
- ☐ Dauern die Auswirkungen voraussichtlich länger als [8] Stunden?
- ☐ Sind Kundschaft, Medien oder Aufsichtsbehörden betroffen?

Bezug zu NIS2: Für Einrichtungen in Sektoren außerhalb der DVO (EU) 2024/2690 gilt ein Cybersicherheitsvorfall nach § 5 Abs. 1 Z 9 NISV 2026 jedenfalls als erheblich, wenn er Krisenmanagement oder Notfallwiederherstellungspläne aktiviert hat (Erläuterungen zu § 5). Ruft eine solche Einrichtung wegen eines Cyberangriffs den Notfall aus, ist sofort die Meldung nach § 34 NISG 2026 zu prüfen. Für Anbieter verwalteter Dienste, Cloud- und Rechenzentrumsdienste und die übrigen DVO-Anbieter gelten stattdessen Art. 3 ff. DVO; dort fehlt dieses Kriterium, die Schwelle von 500 000 Euro oder 5 % des Jahresumsatzes steht aber gleich (Art. 3 Abs. 1 lit. a).

05

Sofortmaßnahmen in den ersten Minuten

Leib und Leben zuerst, dann Schaden eindämmen und Spuren sichern: Checklisten für alle Mitarbeitenden und für die IT.

Sofortmaßnahmen dulden keinen Aufschub. Nach dem BSI-Standard 200-4 müssen sie im Notfallhandbuch dokumentiert sein und Regelungen zum Schutz von Leib und Leben enthalten, der Vorrang vor Sachwerten hat; empfohlen sind Checklisten (Kap. 5.3). Für alle Mitarbeitenden, zum Aushang, nach der IT-Notfallkarte des BSI:

- ☐ Ruhe bewahren und den IT-Notfall sofort melden: [IT-Notfallrufnummer].
- ☐ Angeben: wer meldet, welches System betroffen ist, wie Sie damit gearbeitet haben, was Sie beobachtet haben, wann es passiert ist und wo das System steht.
- ☐ Die weitere Arbeit am betroffenen System einstellen und Beobachtungen dokumentieren.
- ☐ Maßnahmen nur nach Anweisung einleiten.

Für IT-Verantwortliche und Dienstleister, eine Auswahl aus den TOP 12 Maßnahmen bei Cyber-Angriffen von BSI und Partnern; sie ist als Impuls gedacht, die Reihenfolge legen Sie selbst fest:

- Erste Bewertung: Cyberangriff oder technischer Defekt?
- Betroffene Systeme vom Netzwerk und vom Internet trennen, unautorisierte Zugriffe unterbinden.
- Datensicherungen stoppen und vor weiteren Einwirkungen schützen.
- Systemprotokolle, Logdateien, Notizen, Bildschirmfotos und Datenträger forensisch sichern.
- Ausmaß feststellen, alle angegriffenen Systeme identifizieren, zeitkritische Prozesse im Fokus behalten.

- Maßnahmen abstimmen, dokumentieren und allen Verantwortlichen mitteilen; nach Abstimmung Polizei und Behörden benachrichtigen.
- Zugänge betroffener Konten prüfen, etwa neue Passwörter und Zwei-Faktor-Authentisierung.

Empfehlung von TOMORIS: Halten Sie den Zeitpunkt der Kenntnisnahme sofort im Protokoll fest. Gesetzlich laufen ab ihm die Fristen nach § 34 Abs. 2 NISG 2026, nach Art. 33 Abs. 1 DSGVO ab dem Bekanntwerden der Datenschutzverletzung.

06

Wiederanlauf: Reihenfolge und Zielwerte

MTPD, RTO und RPO je System festlegen, die Reihenfolge nach Abhängigkeiten planen und Sicherungen vor dem Einspielen prüfen.

Kenngößen nach BSI-Standard 200-4, Kap. 7 (S. 159 f.)

KENNGRÖSSE	BEDEUTUNG
MTPD, maximal tolerierbare Ausfallzeit	wie lange ein Geschäftsprozess höchstens ausfallen darf, bevor nicht tolerierbare Auswirkungen eintreten; ermittelt in der Business-Impact-Analyse
RTO, geforderte Wiederanlaufzeit	vom Ausrufen des Notfalls bis zur geforderten Inbetriebnahme der Ersatzlösung, etwa dem Zurücksetzen auf den letzten gesicherten Stand; muss kürzer sein als die MTPD, weil die Reaktionszeit davon abgeht
RPO, maximal zulässiger Datenverlust	wie alt die Daten höchstens sein dürfen, um im Notbetrieb sinnvoll zu arbeiten; daraus folgt der Sicherungszyklus
Notbetriebsniveau	wie leistungsfähig der Notbetrieb mindestens sein muss, etwa in Prozent oder als priorisierte Tätigkeiten

Bei NIST SP 800-34 ist die RTO die längste Zeit, die eine Systemressource ausfallen darf, bevor unannehmbare Folgen für andere Ressourcen, die unterstützten Prozesse und die tolerierbare Ausfallzeit (MTD) eintreten (Abschnitt 3.2.1). Legen Sie fest, ab wann Sie die RTO rechnen.

Wiederanlaufreihenfolge zum Ausfüllen (übergeordnete Wiederanlaufplanung, BSI-Standard 200-4, Kap. 12.2)

PRIOR	SYSTEM ODER DIENST	SETZT VORAUS	RTO	RPO
1	_____	_____	____ h	____ h
2	_____	_____	____ h	____ h
3	_____	_____	____ h	____ h
4	_____	_____	____ h	____ h
5	_____	_____	____ h	____ h

Die Reihenfolge richtet sich nach den Abhängigkeiten; die gesamte Wiederanlaufzeit samt abhängigen Ressourcen darf die RTO nicht überschreiten. Im Aufbau- und Standard-BCMS gehört zu jeder zeitkritischen Ressource ein Wiederanlaufplan, so konkret, dass eine fachkundige dritte Person ihn ausführen kann: Geltungsbereich, Zweck und Aktivierung; Rollen und Vertretungen mit aktuellen Kontaktdaten; benötigte Ressourcen mit RTO und Dokumentationen; Voraussetzungen wie Berechtigungen und Dienstleister; die Schritte mit Rolle und üblicher Dauer; ein Funktionstest und die Übergabe in den Notbetrieb (Kap. 12 und 12.2).

Vor dem Einspielen: Sicherungen auf Kompromittierungsindikatoren und Beschädigung prüfen, wiederhergestellte Systeme vor der produktiven Nutzung erneut prüfen und die Ursache beheben (NIST SP 800-61r3, RC.RP-03 und RC.RP-05). Wie Sicherungen im Ernstfall zurückkommen, zeigt die Backup-Checkliste 3-2-1-1-0 auf tomoris.com/downloads.

07

Kommunikation nach innen und außen

Wer was wann erfährt, über welche Kanäle, und welche Meldepflichten parallel laufen.

Legen Sie vorab fest, was Mitarbeitende wann erfahren, was sie gegenüber Presse und in sozialen Medien sagen dürfen, was die Rolle Kommunikation veröffentlicht, wie der Kontakt zu Polizei und Behörden läuft und welche Meldepflichten bestehen (BSI-Standard 200-4, Kap. 5.7.1). Mitarbeitende sollen Informationen spätestens gleichzeitig mit der Öffentlichkeit erhalten (Kap. 5.7.2); für Presseanfragen benennen Sie eine Sprecherin oder einen Sprecher samt Vertretung (Kap. 5.7.3).

Kommunikationsplan zum Ausfüllen (nach dem Beispiel in BSI-Standard 200-4, Tabelle 15)

ZIELGRUPPE	ANLASS	KANAL	ZUSTÄNDIG
Mitarbeitende	laufend während des Notfalls	_____	_____
Kundschaft	bei direkter Betroffenheit	_____	_____
Dienstleister, Lieferanten	bei direkter Betroffenheit	_____	_____
Versicherung	versicherter Schadensfall	_____	_____
Öffentlichkeit, Medien	je nach Szenario und öffentlichem Interesse	_____	_____
Behörden	Meldepflichten, Anzeige	_____	_____

Meldepflichten laufen parallel: Wesentliche und wichtige Einrichtungen melden erhebliche Cybersicherheitsvorfälle dem zuständigen CSIRT, mit Frühwarnung binnen 24 und Meldung binnen 72 Stunden (§ 34 Abs. 2 NISG 2026). Datenschutzverletzungen meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden der Aufsichtsbehörde, außer sie führen voraussichtlich zu keinem Risiko (Art. 33 Abs. 1 DSGVO); einen Vorschlag für 96 Stunden (COM(2025) 837) hat die EU noch nicht beschlossen (Stand 25.10.2026). Details: Leitfaden NIS2-Meldepflichten auf tomoris.com/downloads.

08

Protokoll und Abschluss

Was während der Bewältigung festgehalten wird, eine Protokollvorlage und die Schritte zurück in den Normalbetrieb.

Der Stab protokolliert alle wesentlichen Aktivitäten und Entscheidungen mit Grundlage, Beteiligten, Zeit und Status, Fakten getrennt von Gerüchten (BSI-Standard 200-4, Kap. 5.4). NIS2-Einrichtungen protokollieren die Reaktion und sammeln Nachweise (Anhang Nr. 3.5.4 DVO (EU) 2024/2690); Datenschutzverletzungen sind stets zu dokumentieren (Art. 33 Abs. 5 DSGVO).

Ereignisprotokoll zum Ausfüllen

DATUM, UHRZEIT	MELDUNG, ENTSCHEIDUNG ODER MASSNAHME	WER	STATUS
[TT.MM., hh:mm]	Kenntnisnahme durch [Name]; Meldepflichten prüfen	_____	_____
[TT.MM., hh:mm]	Einstufung als [Störung, Notfall, Krise], Begründung: _____	_____	_____
[TT.MM., hh:mm]	_____	_____	_____

- Notfall beenden: offiziell, nach festgelegten Kriterien, über dieselben Kanäle wie beim Ausrufen (Kap. 5.8); danach Rückstände abarbeiten, Daten nachtragen, auf Hauptsysteme zurückschwenken (Kap. 2.3).
- Auswerten: jeden Vorfall zeitnah und mit Abstand analysieren (Kap. 5.9); ein Abschlussbericht hält Vorfall, Maßnahmen und Lehren fest (NIST SP 800-61r3, RC.RP-06).

09

Übungen und Pflege

Welche Übungen der BSI-Standard vorsieht, wie oft, und wann das Handbuch zu aktualisieren ist.

Ob Pläne funktionieren, zeigen erst Übungen und Tests (BSI-Standard 200-4, Kap. 12.3). Im Reaktiv-BCMS verlangt der Standard regelmäßige Stabs- und Alarmierungsübungen und empfiehlt Planbesprechungen und Funktionstests (Kap. 13.1); die Jahresübungsplanung soll mindestens zwölf Monate umfassen (Kap. 13.3). Wer eine Rolle im Notfallplan hat, soll mindestens jährlich geschult werden (NIST SP 800-34, Abschnitt 3.5.2).

Übungsplan zum Ausfüllen (nach BSI-Standard 200-4, Tabellen 34 und 37)

ÜBUNGSART	WAS GEPRÜFT WIRD	HÄUFIGKEIT	TERMIN
Alarmierungsübung	Erreichbarkeit und Rückrufquote der Alarmierungskette	regelmäßig	_____
Planbesprechung	Pläne plausibel, vollständig und aktuell (Schreibtischtest)	nach Erstellung und wesentlichen Änderungen	_____
Stabsübung	Zusammenarbeit im Stab an einem Szenario	mindestens jährlich	_____
Funktionstest	z. B. Wiederanlauf eines Systems, Lesbarkeit von Sicherungen	jährlich bei RTO unter 24 h, alle 3 Jahre bei RTO unter 5 Tagen	_____

Das Handbuch wird regelmäßig geprüft (DER.4.A1), Kontaktdaten öfter als der Rest, und veraltete Fassungen werden an allen Ablageorten ersetzt (BSI-Standard 200-4, Kap. 4.4.3; NIST SP 800-34, Abschnitt 3.6). Kontaktlisten enthalten personenbezogene Daten und sind zu schützen (NIST SP 800-34, Vorlage in Anhang A.1).

Die Häufigkeiten sind Beispiele des BSI, keine gesetzliche Vorgabe. NIS2-Einrichtungen testen und überprüfen den Notfallplan in geplanten Zeitabständen sowie nach erheblichen Vorfällen oder wesentlichen Änderungen und lassen die Lehren einfließen (Anhang Nr. 4.1.4 DVO (EU) 2024/2690, § 2 NISV 2026). Empfehlung von TOMORIS: Kontaktlisten vierteljährlich prüfen, das ganze Handbuch mindestens einmal im Jahr, und ein aktuelles Exemplar auf Papier außerhalb der eigenen IT aufbewahren.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

NIS2-Betroffenheitscheck
tomoris.com/tools/nis2-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen
tomoris.com/contact
contact@tomoris.com

10

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- BSI-Standard 200-4 Business Continuity Management, Version 1.0 (2023)**
Kap. 2.1, 2.3, 2.6.1, 4.4, 5.1 bis 5.9, 7, 12.2, 12.3 und 13
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Sta...
- BSI IT-Grundschutz-Kompodium, Baustein DER.4 Notfallmanagement, Edition 2023**
Anforderung DER.4.A1 Erstellung eines Notfallhandbuchs
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- BSI: IT-Notfallkarte „Verhalten bei IT-Notfällen“**
www.bsi.bund.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/I...
- BSI und Partner: TOP 12 Maßnahmen bei Cyber-Angriffen, Stand September 2019**
www.bsi.bund.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/T...
- NIST SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems**
Abschnitte 3.2.1, 3.5.2, 3.6, 4.2.2, Vorlage in Anhang A.1
nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-3...
- NIST SP 800-61r3: Incident Response Recommendations (April 2025)**
RC.RP-03, RC.RP-05, RC.RP-06
nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3...
- NISG 2026, BGBl. I Nr. 94/2025, geltende Fassung im RIS**
§ 32 Abs. 4 lit. c, § 34 Abs. 2, Fassung vom 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- NISV 2026, BGBl. II Nr. 290/2026**
§ 2 und § 5 Abs. 1, kundgemacht am 1.10.2026
www.ris.bka.gv.at/eli/bgbII/II/2026/290
- Durchführungsverordnung (EU) 2024/2690, Anhang Nr. 3.5.4, 4.1.2 und 4.1.4**
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu
- Verordnung (EU) 2016/679 (DSGVO), Art. 33 und 34**
Vorschlag COM(2025) 837, Verfahren 2025/0360(COD) offen, Stand 25.10.2026
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- Bundesamt für Cybersicherheit: Erläuterungen zur NISV 2026 (PDF)**
Zu § 5: gilt für Sektoren außerhalb der DVO (EU) 2024/2690
www.bundesamt-cybersicherheit.gv.at/501/files/nisv-2026-erlaeut...