TOMORIS
MORE THAN IT

FREE DOWNLOAD

TEMPLATE · TOMORIS TOOLBOX

IT Emergency Manual: Template for Alerting, Immediate Measures and Recovery

Fillable outline with crisis team, contact list, classification, immediate measures, recovery and exercise plan, backed by BSI Standard 200-4, NIST and the NISG 2026

UPDATED	LENGTH	ONLINE
Oct 25, 2026	PDF, 12 pages	tomoris.com/en/downloads/it-notfallhandbuch-vorlage

AT A GLANCE

3 levels
Disruption, emergency, crisis (BSI Standard 200-4)

7
Tables to fill in, from crisis team to exercise plan

12
Months minimum period of annual exercise planning (BSI)

24 h
NIS2 early warning from becoming aware (§ 34 NISG 2026)

WHO IT IS FOR

- Management of small and medium-sized companies that want to prepare for IT emergencies
- IT managers, information security officers and business continuity officers
- IT service providers who create and practice contingency plans with their customers
- Essential and important entities that must document their contingency plan under the NISG 2026

Adaptation for your own use permitted; redistribute unchanged

WHAT THIS COVERS

In an emergency, there is no time to clarify responsibilities and search for phone numbers. An IT emergency manual brings together in advance what will be needed then: roles, immediate measures, alerting and escalation, as well as communication and recovery plans, as described in the BSI module DER.4. This template provides an outline with sample texts and tables to fill in. It is based on BSI Standard 200-4, the NIST guides SP 800-34 and SP 800-61, and the requirements for contingency plans that have applied since October 2026 to entities under the NISG 2026 (Austrian Network and Information Systems Security Act 2026).

Adapt this template to your company: roles, systems, target values and exercise intervals depend on your business processes. It provides an overview and does not replace legal advice; the text of the law in its current version is decisive.

Usage: You may adapt this template for your own use; you may redistribute it only in unchanged form.

CONTENTS

01 What belongs in the IT emergency manual 3
02 Scope and crisis team 4
03 Alerting and contact list 4
04 Disruption, emergency or crisis 6
05 Immediate measures in the first minutes 7
06 Recovery: order and target values 8
07 Internal and external communication 9
08 Log and closure 10
09 Exercises and maintenance 10
10 Sources 11

01

What belongs in the IT emergency manual

Content according to BSI DER.4, structure according to BSI Standard 200-4, and what is mandatory under the NISG 2026.

In the IT-Grundschutz module DER.4, the BSI describes an emergency manual with information on roles, immediate measures, alerting and escalation, as well as communication, business continuity, recovery and restoration plans. It should record responsibilities and authorities, be accessible even in an emergency and be checked regularly through tests and exercises (DER.4.A1). According to BSI Standard 200-4, the reactive BCMS is suitable as a starting point: first build the response organization and secure selected time-critical processes. Where legal requirements such as the NISG 2026 exist, the BSI recommends starting with the build-up or standard BCMS (ch. 2.6.1).

Content of the contingency plan for NIS2 entities (Annex point 4.1.2 Implementing Regulation (EU) 2024/2690) and where it appears in this template

CONTENT UNDER POINT 4.1.2	SECTION OF THIS TEMPLATE
a) Purpose, scope and audience; b) roles and responsibilities	02 Scope and crisis team
c) Key contacts, internal and external communication channels	03 Alerting, 07 Communication
d) Conditions for activating and deactivating the plan	04 Classification, 08 Log and closure
e) Order of recovery; f) recovery plans with recovery objectives; g) required resources	06 Recovery
h) Resumption of activities after temporary measures	08 Log and closure

For essential and important entities, this is mandatory: § 32 para. 4 lit. c NISG 2026 requires business continuity, such as backup management and disaster recovery, and crisis management; since October 2026, the Annex to Implementing Regulation (EU) 2024/2690, including point 4.1.2, applies to them where appropriate (§ 2 NISV 2026 (Austrian NIS Regulation 2026)). For all other companies, the BSI and NIST requirements are recommendations.

02

Scope and crisis team

What the manual applies to, who sits on the team, who deputizes and what the team may decide without consultation.

Sample text: “This emergency manual applies to [Company] at the sites [Sites] and covers the IT systems and services listed in [Inventory]. It is applied as soon as an event is classified as an emergency or crisis according to Section 04. Version [Number], approved on [MM/DD/YYYY] by [Name, role]; next review on [MM/DD/YYYY]; storage: [digital] and [on paper].” Management approves the structure and staffing of the team (BSI Standard 200-4, ch. 5.1.6).

Crisis team to fill in: roles according to BSI Standard 200-4, ch. 5.1, one deputy per role (ch. 5.1.6)

ROLE AND TASK	PRIMARY (NAME, ROLE)	DEPUTY
Team lead: coordinates the team, generally makes the decisions	_____	_____
IT: technical situation and measures, management of IT service providers	_____	_____
HR as well as buildings and infrastructure	_____	_____
Communication: gather information and prepare it for internal and external audiences	_____	_____
Logging: record events and decisions	_____	_____
As needed: information security, data protection, legal, external experts	_____	_____

> Strategic decisions remain with management; decision-making and financial authority should be delegated to the team (ch. 5.1.1), for example: [shut down systems, engage service providers, expenses up to amount]. One person can take on several roles (ch. 5.1.4); for external members of the team, regulate confidentiality and authority (ch. 5.1.3).

03

Alerting and contact list

From the first indication to an alerted team, with internal and external contact lists to fill in.

1

Detect and report

To the reporting point, e.g. IT hotline [Number]: time and place, reporting person, those affected, possible cause, immediate measures taken, impact, facts separated from assumptions (BSI Standard 200-4, ch. 5.2.1).

2 **Initial assessment**

The reporting point uses simple yes-no questions (Section 04) to check whether an emergency is imminent. When in doubt: better to report too much than too little (ch. 5.2.1).

3 **Decision**

A central, trained and authorized decision-making body, often the team lead, classifies the event and documents the rationale and those involved; the team confirms or downgrades (ch. 5.2.2).

4 **Alert the team**

Briefly and precisely, with a meeting point such as a crisis room or conference call; it is defined who alerts whom through which channels, including outside business hours (ch. 5.2.3).

> Do not alert by email only: with asynchronous channels, it is unclear whether and when the message arrives; calls to mobile phones or alerting apps are better (ch. 5.2.1). Notification procedures during and outside business hours should be documented (NIST SP 800-34, Section 4.2.2). Keep channels ready that work without your own IT (ch. 5.2).

Internal contact list: at least one work number and one private number per person (NIST SP 800-34, template in Appendix A.1)

ROLE	NAME	WORK PHONE	PRIVATE PHONE
Team lead	_____	_____	_____
Deputy team lead	_____	_____	_____
IT owner	_____	_____	_____
Communication	_____	_____	_____
Data protection	_____	_____	_____

External contact list: with contract number and contractual response time (NIST SP 800-34, template in Appendix A.1)

ORGANIZATION	CONTACT PERSON, PHONE	CONTRACT OR CUSTOMER NUMBER	RESPONSE TIME PER CONTRACT
IT service provider	_____	_____	_____
Internet, telephony, cloud, business application	_____	_____	_____
Insurance	_____	_____	_____
CSIRT (report under NISG 2026)	_____	n/a	n/a
Austrian Data Protection Authority (Datenschutzbehörde)	_____	n/a	n/a
Police (criminal complaint)	_____	n/a	n/a

04

Disruption, emergency or crisis

The three levels according to BSI Standard 200-4, guiding questions for the initial assessment and the link to the NIS2 reporting obligation.

Levels according to BSI Standard 200-4, ch. 2.1

LEVEL	CHARACTERISTIC	RESPONSE
Disruption	Processes or resources are not available as intended; can escalate to an emergency if not resolved within a reasonable time	normal organization, such as incident management
Emergency	at least one time-critical business process is interrupted and cannot be restored in normal operations within the maximum tolerable period of disruption; may already be declared when the interruption is imminent	crisis team with existing or adaptable plans
Crisis	damaging event with significant negative impact for which no suitable contingency plans exist or for which they do not work	crisis team, situational

In an event, this means two questions must be answered: Is a time-critical business process affected, and is there an applicable plan? Guiding questions for the IT reporting point based on a BSI example (ch. 5.2.1, Table 10), to be adapted to your processes and worded so that they can be used without in-depth expertise. Sample text: “As soon as any question is answered with yes, notify the team lead immediately: [Name], phone [Number].”

- [ ] Is the affected system part of the security infrastructure, such as antivirus or firewall?
- [ ] Does the outage affect many users or core business operations?
- [ ] Is there a strong suspicion of manipulation of data or systems, data exfiltration, unauthorized exercise of rights or a targeted attack?
- [ ] Is the impact likely to last longer than [8] hours?
- [ ] Are customers, the media or supervisory authorities affected?

Link to NIS2: For entities in sectors outside Implementing Regulation (EU) 2024/2690, a cybersecurity incident under § 5 para. 1 no. 9 NISV 2026 is always considered significant if it has activated crisis management or disaster recovery plans (explanatory notes on § 5). If such an entity declares an emergency because of a cyberattack, the report under § 34 NISG 2026 must be assessed immediately. For managed service providers, cloud and data center services and the other providers covered by the Implementing Regulation, Art. 3 et seq. of the Implementing Regulation apply instead; this criterion is absent there, but the threshold of €500,000 or 5% of annual turnover is the same (Art. 3(1)(a)).

05

Immediate measures in the first minutes

Life and health first, then contain the damage and secure evidence: checklists for all employees and for IT.

Immediate measures cannot be postponed. According to BSI Standard 200-4, they must be documented in the emergency manual and include rules for protecting life and health, which take priority over property; checklists are recommended (ch. 5.3). For all employees, for posting, based on the BSI IT emergency card:

- [ ] Stay calm and report the IT emergency immediately: [IT emergency number].
- [ ] State who is reporting, which system is affected, how you were working with it, what you observed, when it happened and where the system is located.
- [ ] Stop further work on the affected system and document your observations.
- [ ] Take action only when instructed.

For IT owners and service providers, a selection from the TOP 12 measures for cyberattacks by the BSI and partners; it is intended as a prompt, and you define the order yourself:

- Initial assessment: cyberattack or technical defect?
- Disconnect affected systems from the network and the internet, prevent unauthorized access.
- Stop backups and protect them from further interference.
- Forensically secure system logs, log files, notes, screenshots and storage media.
- Determine the extent, identify all attacked systems, keep time-critical processes in focus.
- Coordinate and document measures and communicate them to everyone responsible; after coordination, notify the police and authorities.
- Review access to affected accounts, for example new passwords and two-factor authentication.

> TOMORIS recommendation: record the time of becoming aware in the log immediately. By law, the deadlines under § 34 para. 2 NISG 2026 run from that point, and under Art. 33(1) GDPR from becoming aware of the personal data breach.

06

Recovery: order and target values

Define MTPD, RTO and RPO per system, plan the order by dependencies and check backups before restoring.

Metrics according to BSI Standard 200-4, ch. 7 (p. 159 f.)

METRIC	MEANING
MTPD, maximum tolerable period of disruption	the maximum time a business process may be down before intolerable impacts occur; determined in the business impact analysis
RTO, required recovery time	from the declaration of the emergency to the required commissioning of the replacement solution, such as resetting to the last backed-up state; must be shorter than the MTPD, because the response time is subtracted from it
RPO, maximum acceptable data loss	the maximum age of data that still allows meaningful work in emergency operations; the backup cycle follows from it
Emergency operation level	the minimum performance required in emergency operations, for example as a percentage or as prioritized activities

> In NIST SP 800-34, the RTO is the maximum time a system resource can be unavailable before unacceptable consequences occur for other resources, the supported processes and the maximum tolerable downtime (MTD) (Section 3.2.1). Define from when you calculate the RTO.

Recovery order to fill in (overall recovery planning, BSI Standard 200-4, ch. 12.2)

PRIORITY	SYSTEM OR SERVICE	REQUIRES	RTO	RPO
1	_____	_____	____ h	____ h
2	_____	_____	____ h	____ h
3	_____	_____	____ h	____ h
4	_____	_____	____ h	____ h
5	_____	_____	____ h	____ h

The order follows the dependencies; the total recovery time including dependent resources must not exceed the RTO. In the build-up and standard BCMS, every time-critical resource has a recovery plan that is specific enough for a competent third party to execute: scope, purpose and activation; roles and deputies with current contact details; required resources with RTO and documentation; prerequisites such as permissions and service providers; the steps with role and typical duration; a functional test and the handover to emergency operations (ch. 12 and 12.2).

Before restoring: check backups for indicators of compromise and damage, check restored systems again before productive use and fix the root cause (NIST SP 800-61r3, RC.RP-03 and RC.RP-05). The backup checklist 3-2-1-1-0 at tomoris.com/downloads shows how backups come back in an emergency.

07

Internal and external communication

Who learns what and when, through which channels, and which reporting obligations run in parallel.

Define in advance what employees learn and when, what they may say to the press and on social media, what the communication role publishes, how contact with the police and authorities works and which reporting obligations exist (BSI Standard 200-4, ch. 5.7.1). Employees should receive information no later than the public does (ch. 5.7.2); for press inquiries, appoint a spokesperson and a deputy (ch. 5.7.3).

Communication plan to fill in (based on the example in BSI Standard 200-4, Table 15)

AUDIENCE	OCCASION	CHANNEL	RESPONSIBLE
Employees	ongoing during the emergency	_____	_____
Customers	if directly affected	_____	_____
Service providers, suppliers	if directly affected	_____	_____
Insurance	insured loss event	_____	_____
Public, media	depending on the scenario and public interest	_____	_____
Authorities	reporting obligations, criminal complaint	_____	_____

Reporting obligations run in parallel: essential and important entities report significant cybersecurity incidents to the competent CSIRT, with an early warning within 24 hours and a notification within 72 hours (§ 34 para. 2 NISG 2026). The controller reports personal data breaches to the supervisory authority without undue delay and, where feasible, within 72 hours, unless they are unlikely to result in a risk (Art. 33(1) GDPR); the EU has not yet adopted a proposal for 96 hours (COM(2025) 837) (as of October 25, 2026). Details: NIS2 reporting obligations guide at tomoris.com/downloads.

08

Log and closure

What is recorded during the response, a log template and the steps back to normal operations.

The team logs all significant activities and decisions with basis, participants, time and status, keeping facts separate from rumors (BSI Standard 200-4, ch. 5.4). NIS2 entities log the response and collect evidence (Annex point 3.5.4 Implementing Regulation (EU) 2024/2690); personal data breaches must always be documented (Art. 33(5) GDPR).

Event log to fill in

DATE, TIME	REPORT, DECISION OR MEASURE	WHO	STATUS
[MM/DD, hh:mm]	Became aware: [Name]; assess reporting obligations	_____	_____
[MM/DD, hh:mm]	Classified as [disruption, emergency, crisis], rationale: _____	_____	_____
[MM/DD, hh:mm]	_____	_____	_____

- End the emergency: officially, according to defined criteria, through the same channels used to declare it (ch. 5.8); then work through backlogs, enter missing data and switch back to primary systems (ch. 2.3).
- Evaluate: analyze every incident promptly and with some distance (ch. 5.9); a final report records the incident, measures and lessons learned (NIST SP 800-61r3, RC.RP-06).

09

Exercises and maintenance

Which exercises the BSI standard provides for, how often, and when the manual needs to be updated.

Only exercises and tests show whether plans work (BSI Standard 200-4, ch. 12.3). In the reactive BCMS, the standard requires regular crisis team and alerting exercises and recommends plan reviews and functional tests (ch. 13.1); annual exercise planning should cover at least twelve months (ch. 13.3). Anyone with a role in the contingency plan should be trained at least annually (NIST SP 800-34, Section 3.5.2).

Exercise plan to fill in (based on BSI Standard 200-4, Tables 34 and 37)

EXERCISE TYPE	WHAT IS TESTED	FREQUENCY	DATE
Alerting exercise	Reachability and callback rate of the alerting chain	regularly	_____
Plan review	Plans plausible, complete and current (desk check)	after creation and significant changes	_____
Crisis team exercise	Collaboration within the team on a scenario	at least annually	_____

Functional test	e.g. recovery of a system, readability of backups	annually for an RTO under 24 h, every 3 years for an RTO under 5 days	_____

The manual is reviewed regularly (DER.4.A1), contact details more often than the rest, and outdated versions are replaced at all storage locations (BSI Standard 200-4, ch. 4.4.3; NIST SP 800-34, Section 3.6). Contact lists contain personal data and must be protected (NIST SP 800-34, template in Appendix A.1).

> The frequencies are BSI examples, not legal requirements. NIS2 entities test and review the contingency plan at planned intervals and after significant incidents or significant changes, and incorporate the lessons learned (Annex point 4.1.4 Implementing Regulation (EU) 2024/2690, § 2 NISV 2026). TOMORIS recommendation: review contact lists quarterly and the entire manual at least once a year, and keep a current paper copy outside your own IT.

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

NIS2 applicability check (German)
tomoris.com/tools/nis2-check

DISCUSS IMPLEMENTATION

Get in Touch
tomoris.com/en/contact

contact@tomoris.com

10

Sources

All statements are supported by sources. Legislation applies in its current version.

1 **BSI Standard 200-4 Business Continuity Management, version 1.0 (2023)**
Ch. 2.1, 2.3, 2.6.1, 4.4, 5.1 to 5.9, 7, 12.2, 12.3 and 13
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Sta...

2 **BSI IT-Grundschutz-Kompendium, module DER.4 Business Continuity Management, Edition 2023**
Requirement DER.4.A1 creating an emergency manual
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...

3 **BSI: IT emergency card “Behavior in IT emergencies”**
www.bsi.bund.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/I...

4 **BSI and partners: TOP 12 measures for cyberattacks, as of September 2019**
www.bsi.bund.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/T...

5 **NIST SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems**
Sections 3.2.1, 3.5.2, 3.6, 4.2.2, template in Appendix A.1
nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-3...

6 **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....

7 **NISG 2026, BGBl. I No. 94/2025, current version in the RIS**
§ 32 para. 4 lit. c, § 34 para. 2, version of October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...

8 **NISV 2026, BGBl. II No. 290/2026**
§ 2 and § 5 para. 1, promulgated on October 1, 2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290

9 **Implementing Regulation (EU) 2024/2690, Annex**
Points 3.5.4, 4.1.2 and 4.1.4
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu

10 **Regulation (EU) 2016/679 (GDPR), Art. 33 and 34**
Proposal COM(2025) 837, procedure 2025/0360(COD) pending, as of October 25, 2026
eur-lex.europa.eu/eli/reg/2016/679/oj/deu

11 **Federal Office for Cybersecurity: explanatory notes on the NISV 2026 (PDF)**
On § 5: applies to sectors outside Implementing Regulation (EU) 2024/2690
www.bundesamt-cybersicherheit.gv.at/501/files/nisv-2026-erlaeut...