

CHEAT SHEET · TOMORIS TOOLBOX

IT Emergency Card: A Fill-In Poster for When Things Go Wrong

One page to post with emergency numbers, reporting questions and rules of conduct, plus reporting bodies in Austria and the first questions for IT

UPDATED

Oct 25, 2026

LENGTH

PDF, 7 pages

ONLINE

tomoris.com/en/downloads/it-notfallkarte

AT A GLANCE

1 page

to fill in and post

6

questions answered
when reporting

3

rules of conduct for all
employees

12

questions for IT after a cy-
berattack

WHO IT IS FOR

- All employees, for whom the card hangs at workstations and in hallways
- IT management and emergency managers who fill in and roll out the card
- Management of small and medium-sized businesses without their own IT department
- IT service providers who prepare emergency cards for their customers

WHAT THIS COVERS

In an IT emergency, the first minutes count. Anyone who notices that something is wrong must know whom to call, what to say and what to leave alone. This emergency card follows the poster “Behavior in IT Emergencies” from the German Federal Office for Information Security (BSI) and adapts it to Austria. Page 3 is the card to fill in and post. The other pages explain how to fill it in and roll it out, which bodies you can reach in Austria and which questions IT should ask after an attack.

This emergency card is a TOMORIS recommendation based on the sources listed and must be adapted to your business. Third-party contact details reflect the status as of October 25, 2026, as stated by the respective bodies. It does not replace an emergency manual or legal advice on reporting obligations.

CONTENTS

01	How to use this card	2
02	What to do in an IT emergency	3
03	How to fill in and roll out the card	4
04	External bodies in Austria	4
05	For IT: twelve questions after a cyberattack	5
06	Sources	6

01 —

How to use this card

The next page is the poster. Fill it in, print it and post it where employees will look in an emergency.

The BSI sees its IT emergency card as a sign similar to the well-known “What to do in case of fire” poster. It puts three messages first: know the contacts for IT emergencies and how to reach them, pass on key information immediately, and take countermeasures only after consultation or on instruction. It is often hard to tell whether a malfunction or an attack has occurred. That decision should rest with the responsible people, not with the person who notices the emergency.

Print the next page on its own after filling in the fields: emergency numbers, availability and your decision on disconnecting from the network. Alternatively, create the card with the IT Emergency Card tool on tomoris.com using your own contacts and print it in A4. The pages after it are meant for emergency managers and IT.

02 —

What to do in an IT emergency

Stay calm and report immediately. Better to call once too often than once too few.

Whom to call

WHO	PHONE	AVAILABLE
IT emergency number	_____	_____
Deputy	_____	_____
IT service provider	_____	_____
Management	_____	_____

What to say on the phone

Who is reporting?	Name, department, callback number.
Which device?	Which computer, program or service is affected?
What did you do?	How did you last work with it, for example by opening an attachment?
What did you see?	Messages, locked files, unusual behavior.
When?	The time you noticed it.
Where?	Building, room, workstation.

- ☐ Stop working on the affected device
- ☐ Write down what you observed, photograph the screen with your work phone
- ☐ Take action only on instruction from the IT emergency number
- ☐ If you suspect malware: [unplug the network cable and turn off Wi-Fi] or [only on instruction]

Do not repair anything yourself, do not delete anything, do not make any payments. If people are in danger: police emergency number 133 or European emergency number 112.

03

How to fill in and roll out the card

For emergency managers and IT: enter the numbers, make one decision, post, train, review.

1 Set the emergency number

Enter a number that someone answers in an emergency, internally or at your IT service provider, plus a deputy. The BSI provides a field for the individual phone number on its card for this purpose.

2 Decide on network disconnection

Decide whether employees who suspect malware should unplug cables and turn off Wi-Fi themselves. In case of ransomware, the Austrian Federal Criminal Police Office (Bundeskriminalamt) advises businesses to disconnect affected systems from the network immediately. The BSI advises employees to take action only on instruction. The card makes your decision unambiguous.

3 Post it

In hallways, offices, workshops and at IT workstations, wherever employees should find it in an emergency (BSI). For employees who speak other languages, the BSI offers the card in ten more languages.

4 Introduce it in training

The BSI recommends presenting the card as part of training and awareness programs and encouraging employees to report anything unusual.

5 Keep it up to date

Check the numbers whenever staff or service providers change, and at least every six months. Once a year, make a test call outside office hours. This is a TOMORIS recommendation.

The BSI expressly allows organizations to copy and distribute its own card and fill in the fields. This TOMORIS card follows its content but is a separate version for Austria.

04

External bodies in Austria

For emergency managers: whom to involve and when. Details as stated by the bodies themselves, as of October 25, 2026.

Reporting bodies and help with IT emergencies in Austria

BODY	WHEN	CONTACT AS STATED BY THE BODY
Police emergency number, European emergency number	In case of imminent danger or when the police are needed on site	133, 112

Police station	Reporting a crime, for example after an attack or extortion	any police station; service number 059-133
Cybercrime reporting office at the Federal Criminal Police Office	Suspected cybercrime, help and information; you currently cannot file a criminal complaint this way	against-cybercrime@bmi.gv.at
CERT.at	Reporting IT security incidents; not a general IT help desk	reports@cert.at, +43 1 5056416-78, Mon–Fri 8 a.m.–6 p.m. on working days
Cyber Security Hotline of the Austrian Economic Chambers	Initial information by phone and emergency help for members	0800 888 133, daily 24 hours
Austrian Data Protection Authority (Datenschutzbehörde)	Personal data breach: without undue delay, where feasible within 72 hours (Art. 33 GDPR)	see the Data Protection Authority website
Competent CSIRT, NIS2 entities only	Significant cybersecurity incident: early warning within 24 hours (§ 34 para. 2 no. 1 NISG 2026, Austrian Network and Information Systems Security Act 2026)	sector-specific CSIRT, otherwise national CSIRT

Whether a reporting obligation exists under the GDPR or the NISG 2026 is decided by management together with the emergency managers, not by the person reporting. When filling in the card, check phone numbers and availability on the bodies' websites.

05

For IT: twelve questions after a cyberattack

Based on "TOP 12 Measures in Case of Cyberattacks" by the BSI, the German Federal Criminal Police Office and partners, as a prompt, not a fixed sequence.

- ☐ Initial assessment: cyberattack or technical fault?
- ☐ Measures continuously coordinated, documented and communicated to everyone responsible?
- ☐ Logs, log files, notes, photos of screens and storage media secured forensically?
- ☐ Particularly time-critical business processes in focus?
- ☐ Affected systems and their internet connections disconnected, unauthorized access stopped?
- ☐ Backups stopped and protected from further interference?
- ☐ Extent of the spread determined, all attacked systems identified?

- ☐ Exploited vulnerabilities in systems and processes fixed?
- ☐ Police and authorities notified after coordination (data protection, reporting obligations)?
- ☐ Access rights and sign-in methods of affected accounts reviewed, for example new passwords and two-factor sign-in?
- ☐ Network monitored further after the incident?
- ☐ Affected data and systems restored or rebuilt?

The publishers stress that handling a cyberattack is always individual. The measures must be adapted to the IT, the type of attack and the goals of the organization (TOP 12, as of September 2019). An IT emergency manual helps with planning in advance.

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

IT emergency card (German)

tomoris.com/tools/notfallkarte

NIS2 reporting deadline calculator (German)

tomoris.com/tools/meldefristen-rechner

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

06

Sources

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

- 1 **BSI: IT emergency card "Behavior in IT Emergencies" (DIN A4)**
Reporting questions and rules of conduct
www.bsi.bund.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/...
- 2 **BSI: IT emergency card, usage notes and terms of use**
Messages, posting locations, training, languages, terms of use
www.bsi.bund.de/dok/13035678
- 3 **BSI and partners: TOP 12 Measures in Case of Cyberattacks, as of September 2019**
twelve questions, preliminary remarks
www.bsi.bund.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/T...
- 4 **Federal Criminal Police Office: Ransomware, information for businesses in Austria (v20260806)**
"And if it has happened ..."
www.bundeskriminalamt.at/212/service/files/ransomware/324_2026...
- 5 **Federal Criminal Police Office: Cybercrime, reporting office against Cybercrime**
last updated August 27, 2026
www.bundeskriminalamt.at/306/start.html
- 6 **Police: Emergency numbers**
133, 112, service number 059-133
www.polizei.gv.at/alle/notrufe.aspx
- 7 **CERT.at: Contact**
Reporting security incidents, availability
www.cert.at/de/ueber-uns/kontakt
- 8 **WKO: Cyber Security Hotline of the Austrian Economic Chambers**
Phone number, availability, for members
www.wko.at/it-sicherheit/cyber-security-hotline

9 Regulation (EU) 2016/679 (GDPR), Art. 33

Notification to the supervisory authority
eur-lex.europa.eu/eli/reg/2016/679/oj/deu

10 NISG 2026, BGBl. I No. 94/2025, version in force in the RIS

§ 34 paras. 1 and 2, version of October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...