

GUIDE · TOMORIS TOOLBOX

# Incident Response: Security Incident Playbook for SMBs

Phases, roles, decisions with criteria, reporting deadlines and incident log, based on NIST SP 800-61 Rev. 3, BSI DER.2.1 and the CISA playbooks

UPDATED

Oct 25, 2026

LENGTH

PDF, 9 pages

ONLINE

[tomoris.com/en/downloads/incident-response-playbook](https://tomoris.com/en/downloads/incident-response-playbook)

AT A GLANCE

**24 h**

early warning for significant incidents (NISG 2026)

**72 h**

notification to the CSIRT and the Data Protection Authority

**6**

NIST CSF 2.0 functions in the model

**1**

Consider an incident lead per incident (NIST RS.MA-01)

WHO IT IS FOR

- IT management and administrators who handle incidents technically
- Information security officers who coordinate the response
- Management deciding on shutdown, notification and communication
- IT service providers who support customers during incidents

## WHAT THIS COVERS

A security incident leaves no time to sort out responsibilities first. This playbook structures the handling of every incident, from a hijacked account to data exfiltration: which phases you follow, who has which role, which decisions are due and the criteria for making them, which reporting deadlines are running and how to log everything traceably. It is based on NIST SP 800-61 Rev. 3, module DER.2.1 of the BSI IT-Grundschutz Compendium (IT baseline protection of the German Federal Office for Information Security) and the playbooks of the US agency CISA. Immediate measures for ransomware, the emergency manual and the NIS2 notification are covered in separate downloads.

This guide is a TOMORIS recommendation and replaces neither a contingency plan nor legal advice or forensic support. Adapt roles, contacts and criteria to your business. Whether a reporting obligation exists depends on your entity and the incident; the NISG 2026, the NISV 2026 and the GDPR as currently in force are authoritative.

### CONTENTS

|           |                                           |          |
|-----------|-------------------------------------------|----------|
| <b>01</b> | What a playbook must deliver .....        | <b>2</b> |
| <b>02</b> | The phases at a glance .....              | <b>3</b> |
| <b>03</b> | Roles during an incident .....            | <b>4</b> |
| <b>04</b> | Step-by-step process .....                | <b>5</b> |
| <b>05</b> | Decisions with criteria .....             | <b>6</b> |
| <b>06</b> | Keeping reporting deadlines in view ..... | <b>7</b> |
| <b>07</b> | Incident log to fill in .....             | <b>7</b> |
| <b>08</b> | Post-incident review and exercises .....  | <b>8</b> |
| <b>09</b> | Sources .....                             | <b>9</b> |

## 01 —

# What a playbook must deliver

Why incident handling must be prepared and what the BSI requires

NIST describes how incidents have changed: they are more frequent and cause more damage, and recovery often takes weeks or months. Incident handling therefore belongs in overall risk management (SP 800-61 Rev. 3, Section 2.1). Playbooks provide actionable steps for typical situations; documented procedures can be practiced and help onboard new people (Section 2.3).

### BSI basic requirements (DER.2.1, Edition 2023)

|                         |                                                                                                                                                                        |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DER.2.1.A1</b>       | Clearly define what a security incident is and distinguish it from disruptions in day-to-day operations; everyone involved knows the definition.                       |
| <b>DER.2.1.A2</b>       | Policy for handling security incidents with rules of conduct for each type of incident, adopted by management, known to everyone, updated regularly.                   |
| <b>DER.2.1.A3</b>       | Define responsibilities and contacts, including who decides on a forensic investigation, by which criteria and when; contact details up to date and easily accessible. |
| <b>DER.2.1.A4 to A6</b> | Inform affected parties promptly and observe reporting obligations, contain and resolve the incident, restore the operating environment securely.                      |

This playbook is a TOMORIS recommendation for the general process for any type of security incident. Immediate measures for ransomware, the emergency manual for recovery and the form for the NIS2 notification are in separate downloads.

## 02

# The phases at a glance

From the familiar phase model to the model based on NIST CSF 2.0

### Phases of incident handling (previous NIST model, with containment separate as in the CISA playbook)



Rev. 3 maps incident handling to the six functions of the NIST Cybersecurity Framework 2.0: Govern, Identify and Protect prepare, while Detect, Respond and Recover are the actual handling; findings flow back continuously through the Improvement category. NIST expressly leaves it to each organization to use the model that suits it. This playbook uses the familiar phases and lists the identifiers from Rev. 3.

03 —

## Roles during an incident

Who decides, who handles, who informs

Roles according to NIST SP 800-61 Rev. 3 (Section 2.2) and BSI DER.2.1

| ROLE                                     | TASK DURING THE INCIDENT                                                                                                                                                  |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Executive management</b>              | Oversees the response, provides resources and decides on high-impact steps such as shutting down or rebuilding important services.                                        |
| <b>Incident lead</b>                     | One person per incident who leads the response, assigns tasks and keeps the log (NIST RS.MA-01: incident lead).                                                           |
| <b>Technical staff and IT operations</b> | Check whether an incident has occurred, collect and analyze data, contain, find the cause, restore. The head of IT operations approves remediation measures (DER.2.1.A5). |
| <b>Data protection, legal</b>            | Review reporting obligations, contracts and legal consequences; whether to involve the data protection officers must be assessed (DER.2.1.A4).                            |
| <b>Communications</b>                    | Coordinates statements to employees, customers and the media; only authorized people pass on information (DER.2.1.A9).                                                    |
| <b>HR, works council</b>                 | HR is involved if employees are suspected of having caused an incident intentionally (NIST 2.2); whether to involve the works council must be assessed (DER.2.1.A4).      |
| <b>External parties</b>                  | IR service providers, cloud and internet providers with contractually defined tasks, rights and information channels (NIST 2.2).                                          |

Contacts for the incident (to fill in, keep up to date and easily accessible)

| ROLE                        | NAME  | REACHABLE AT | DEPUTY |
|-----------------------------|-------|--------------|--------|
| <b>Incident lead</b>        | _____ | _____        | _____  |
| <b>Executive management</b> | _____ | _____        | _____  |
| <b>IT operations</b>        | _____ | _____        | _____  |
| <b>Data protection</b>      | _____ | _____        | _____  |
| <b>IR service provider</b>  | _____ | _____        | _____  |
| <b>Competent CSIRT</b>      | _____ | _____        | _____  |

04 —

## Step-by-step process

From the first report to confirmed normal operations

### 1 Receive and review the report

Reports come in through fixed, trusted channels (DER.2.1.A9), including from third parties (NIST RS.MA-02). Briefly check whether a security incident has actually occurred and estimate severity and urgency (NIST RS.MA-02).

### 2 Declare the incident, appoint a lead

If the defined criteria are met, declare the incident and appoint a responsible person; if needed, call in the IR service provider and trigger other plans such as the contingency plan (NIST DE.AE-08, RS.MA-01).

### 3 Classify and prioritize

Determine the type of incident, such as data exfiltration, ransomware, account takeover or service outage, and classify and prioritize it using a consistent method (NIST RS.MA-03, DER.2.1.A11).

### 4 Log and secure evidence

Record every finding and action with a timestamp, keep records confidential and unaltered; secure data that can explain the type and cause (NIST RS.AN-06, RS.AN-07; DER.2.1.A6, A16).

### 5 Contain

Isolate affected systems and network segments, block unauthorized access, change passwords, keys and service accounts if compromise is suspected, revoke privileged access (CISA playbook, Containment). Weigh the impact on operations and on evidence preservation.

### 6 Determine extent and cause

Reconstruct the sequence of events, identify vulnerabilities and attack paths, and search for traces and backdoors even on systems that are not obviously affected (NIST RS.AN-03, RS.AN-08). New traces expand the analysis and containment (CISA playbook).

### 7 Eradicate

Identify all affected systems and services, remove malware, disable compromised accounts, close exploited vulnerabilities (NIST RS.MI-02); have the head of IT operations approve the measures beforehand (DER.2.1.A5).

### 8 Recover and confirm

Check backups for integrity before use (NIST RC.RP-03), restore systems with all patches, change all credentials, involve users in functional tests and then monitor closely (DER.2.1.A6). Declare the end of the incident based on criteria (NIST RC.RP-06).

Do not tip off the attacker: CISA advises informing affected parties by phone rather than email, using a channel outside the potentially compromised systems for coordination and not uploading malware samples to public analysis services.

## 05

# Decisions with criteria

The key decision points and who makes them

## Decisions during an incident (assignment of “who”: TOMORIS recommendation)

| DECISION                                       | CRITERIA ACCORDING TO SOURCE                                                                                                                                                                                                            | WHO                                                           |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| <b>Contain immediately or keep observing?</b>  | Whether limiting damage or investigation is more important (DER.2.1.A10); impact on operations, duration and effectiveness, impact on evidence; risk of alerting the attacker versus risk of leaving them in the network longer (CISA). | Incident lead with executive management                       |
| <b>Disconnect systems, shut down services?</b> | According to NIST, management can decide on high-impact steps such as shutting down or rebuilding important services (NIST 2.2); take affected components off the network (DER.2.1.A6).                                                 | Executive management                                          |
| <b>Bring in forensics?</b>                     | Define criteria and responsibility in advance (DER.2.1.A3); evidence preservation with chain of custody, for example if prosecution is possible (NIST RS.AN-07).                                                                        | Executive management on the recommendation of technical staff |
| <b>Report to authorities?</b>                  | Check statutory reporting obligations (DER.2.1.A4); NISG 2026, GDPR; police according to the criteria in the plan and with management approval (NIST RS.CO-02).                                                                         | Executive management, data protection                         |
| <b>Inform customers and the public?</b>        | Inform recipients of the services without undue delay if they are affected (§ 34 para. 3 NISG 2026); data subjects in case of high risk (Art. 34 GDPR); public statements only through approved channels (NIST RC.CO-04).               | Executive management, communications                          |
| <b>Start recovery?</b>                         | Apply defined criteria for starting recovery, taking possible operational disruptions into account (NIST RS.MA-05).                                                                                                                     | Incident lead, IT operations                                  |

06 —

## Keeping reporting deadlines in view

What runs for significant incidents and personal data breaches

**Reporting deadlines: 24 and 72 hours from becoming aware, final report from notification**



### 24 hours

#### Early warning to the CSIRT

Without undue delay, at the latest within 24 hours: for essential and important entities in case of significant cybersecurity incidents (§ 34 para. 2 no. 1 NISG 2026).



### 72 hours

#### Notification to the CSIRT and the Data Protection Authority

Notification with an initial assessment to the CSIRT (§ 34 para. 2 no. 2 NISG 2026); for personal data breaches, to the Austrian Data Protection Authority (Datenschutzbehörde) without undue delay and, where feasible, within 72 hours (Art. 33(1) GDPR).



### 1 month

#### Final report

No later than one month after the notification. If the incident is still ongoing, first a progress report, and then the final report within one month after incident handling ends (§ 34 para. 2 nos. 4 and 5 NISG 2026).

Under § 35 para. 1 NISG 2026, an incident is significant if it has caused or is capable of causing severe operational disruption or financial loss for the entity, or has affected or is capable of affecting others by causing considerable material or non-material damage; the NISV 2026 (Austrian NIS Regulation 2026) sets out further criteria. The GDPR notification is only waived if the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Check both obligations in parallel and early. The fields and process of the NIS2 notification are in the “NIS2 incident report” template, and the obligations are in the “NIS2 reporting obligations” guide.

07 —

## Incident log to fill in

Master data and diary of the incident, keep confidential

### Incident master data

| FIELD                                                                         | ENTRY |
|-------------------------------------------------------------------------------|-------|
| Incident number                                                               | _____ |
| Detected on, at, by                                                           | _____ |
| Incident lead                                                                 | _____ |
| Type (data exfiltration, ransomware, account takeover, service outage, other) | _____ |
| Affected systems, services, data                                              | _____ |

NISG 2026 reporting obligation checked on, result

\_\_\_\_\_

GDPR reporting obligation checked on, result

\_\_\_\_\_

End of incident declared on, by

\_\_\_\_\_

Diary: every finding and action with a timestamp (NIST RS.AN-06, DER.2.1.A16)

| DATE, TIME | OBSERVATION OR ACTION | DECISION | WHO   |
|------------|-----------------------|----------|-------|
| _____      | _____                 | _____    | _____ |
| _____      | _____                 | _____    | _____ |
| _____      | _____                 | _____    | _____ |
| _____      | _____                 | _____    | _____ |
| _____      | _____                 | _____    | _____ |
| _____      | _____                 | _____    | _____ |

## 08

# Post-incident review and exercises

Learn from every incident and practice the process

- ☐ Final report prepared: incident, handling and recovery measures, lessons learned (NIST RC.RP-06).
- ☐ Evaluated: how quickly was the incident detected and resolved, did the reporting channels work, was the information sufficient, were detection and measures effective (DER.2.1.A17)?
- ☐ Everyone involved has reported their experiences; processes and procedures adjusted (DER.2.1.A18).
- ☐ Cause eliminated, vulnerabilities in infrastructure and processes recorded, roles and authorities clarified, training needs and tools improved (CISA, Post-Incident).
- ☐ Detection sharpened: rules and logging for the observed attack techniques added, blind spots closed (CISA, Post-Incident).
- ☐ Executive management informed: annually about all incidents, immediately if urgent action is needed (DER.2.1.A17).
- ☐ Instructions for comparable incidents created and communicated (DER.2.1.A17).
- ☐ Escalation paths tested in exercises (DER.2.1.A14), and tabletop exercises for increased protection needs (A22); lessons from exercises incorporated (NIST ID.IM-02).

- ☐ Playbook and contacts reviewed and updated regularly (DER.2.1.A7, NIST ID.IM-04).

#### NEXT STEP

## Check It Yourself or Put It into Practice Together

#### CHECK FOR FREE

##### IT emergency card

[tomoris.com/en/tools/notfallkarte](https://tomoris.com/en/tools/notfallkarte)

##### NIS2 reporting deadline calculator

[tomoris.com/en/tools/meldefristen-rechner](https://tomoris.com/en/tools/meldefristen-rechner)

#### DISCUSS IMPLEMENTATION

##### Get in Touch

[tomoris.com/en/contact](https://tomoris.com/en/contact)

[contact@tomoris.com](mailto:contact@tomoris.com)

## 09

## Sources

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

- NIST SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management (April 2025)**  
Sections 2.1 to 2.3, table of CSF categories DE, RS, RC and ID.IM, accessed October 25, 2026  
[nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3...](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3...)
- BSI IT-Grundschutz Compendium, module DER.2.1 Handling of Security Incidents (Edition 2023)**  
Requirements A1 to A22, accessed October 25, 2026  
[www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...)
- CISA: Cybersecurity Incident & Vulnerability Response Playbooks (November 2021)**  
Incident Response Playbook: preparation, containment, post-incident activity, accessed October 25, 2026  
[www.cisa.gov/sites/default/files/publications/Federal\\_Governmen...](https://www.cisa.gov/sites/default/files/publications/Federal_Governmen...)
- NISG 2026, BGBl. I No. 94/2025, version in force in the RIS**  
§ 34 reporting obligations, § 35 significant cybersecurity incident, accessed October 25, 2026  
[www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...](https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...)
- NISV 2026, BGBl. II No. 290/2026**  
§§ 5 to 7 significance, accessed October 25, 2026  
[www.ris.bka.gv.at/eli/bgbl/II/2026/290](https://www.ris.bka.gv.at/eli/bgbl/II/2026/290)
- Regulation (EU) 2016/679 (GDPR), German version on EUR-Lex**  
Art. 33 and 34, accessed October 25, 2026  
[eur-lex.europa.eu/eli/reg/2016/679/oj/deu](https://eur-lex.europa.eu/eli/reg/2016/679/oj/deu)