CHECKLIST 20 REVIEW POINTS 9 MIN REVIEWED 10/08/2026

Managing IT security incidents organizationally

First organizational steps for roles, situation report, communication, evidence and restart in the event of a suspected IT security incident.

FOR WHOM

Management, IT, information security, data protection and communication in small and medium-sized companies.

WHEN TO USE IT

Immediately upon a suspected incident and in parallel with expert technical analysis.

THE SHORT ANSWER

In the event of a suspected IT security incident, what counts is calm, a named operations management, a secure situation report, coordinated technical measures, documented decisions and timely checked reporting and communication obligations.

Important boundary: In the event of acute danger, ongoing blackmail or failure of critical systems, immediately contact appropriate internal and external specialist departments. Do not delete evidence or make uncoordinated changes.

01 Leadership and accessibility

A small group capable of acting is better than many parallel individual decisions.

- [ ] **Keep calm and name operations management**

  A reachable person coordinates decisions, tasks and timeline.

- [ ] **Activate necessary internal roles**

  IT, information security, management, data protection and communication are included as appropriate to the incident.

- [ ] **Use an independent communication channel**

  If the company network may be affected, contacts and coordination will be organized outside of this network.

- [ ] **Check external support**

  Incident response, forensics, insurers, legal advice and relevant authorities will be contacted as necessary.

02 Situation report and evidence

Early observations and timing are crucial later for technology, duties and communication.

- [ ] **Collect known observations**

  Who noticed which behavior, when, and which systems and users are affected?

- [ ] **Begin timeline**

  Continuously document observations, decisions, actions taken and responsible persons.

- [ ] **Protect logs and evidence**

  Data is not hastily deleted, cleaned or overwritten. Expert security takes priority.

- [ ] **Assess damage spread**

  Affected accounts, devices, locations, data, and dependent services will be progressively isolated.

03 Coordinate containment

Emergency technical measures must limit damage without unnecessarily jeopardizing evidence or recovery.

- [ ] **Technically approve measures**

  Isolation, blocking or shutdown are carried out based on the situation report and with a documented decision.

- [ ] **Secure privileged access**

  Suspicious sessions, administrator access and remote access are handled in a controlled manner.

- [ ] **Consider dependencies**

  Before shutdowns, the effects on production, safety and restarts are examined.

- [ ] **Control effectiveness**

  After each measure, it is checked whether the situation, spread or evidence has changed.

04 Reporting and communication

Unverified statements create additional harm. However, deadlines should not be overlooked.

- [ ] **Check possible reporting requirements**

  Data protection, NIS2, contracts, insurance and industry-specific requirements are assessed with responsible specialist advice.

- [ ] **Establish uniform language regulations**

  Confirmed facts, uncertainties and next update are clearly separated.

- [ ] **Identify affected groups**

  Employees, customers, partners, authorities and the public are only informed according to the situation.

- [ ] **Process inquiries centrally**

  A notified body prevents contradictory information and documents outgoing information.

05 Restart and follow-up

A system is not trustworthy simply because it can be accessed again.

- [ ] **Confirm clean recovery base**

  Cause, accounts, configuration, backups and known persistence are checked before the restart.

- [ ] **Start prioritized services gradually**

  Critical processes receive a defined sequence, acceptance criteria and increased monitoring.

- [ ] **Renew affected access and secrets**

  Passwords, keys, tokens and certificates are treated risk-based.

- [ ] **Implement findings in a binding manner**

  Causes, effective measures, open risks, responsible persons and dates are recorded after the incident.

Result of the joint review

- A named operational management and clear roles
- A continuous situation report with a timeline
- Coordinated technical and communication decisions
- A tested restart with follow-up

Related guidance

- Incident response plan for medium-sized businesses →
- Cybersecurity →
- sudo/PORT security understanding →

Sources and professional basis

This working aid translates general recommendations into a compact initial review. The primary sources and your specific context remain decisive.

- BSI: Incident, organizational checklist →
- BSI: Incident Support →

Frequently asked questions

Should an affected system be switched off immediately?

Does this list replace an incident response plan?

Browser checkmarks are not stored or transmitted to sudo/PORT.