Incident response checklist and forms

Edition 16 November 2026. Free to copy and adapt under CC BY 4.0. Fields in [square brackets] are for you to fill in.

First-hours checklist

Tick each item and write the time. Hand the page to the next shift with the log.

Step	Done	Time	By
Incident declared. Severity set. Log opened.	[ ]		
Incident lead, technical lead and communications lead called.	[ ]		
Out-of-band channel opened (phone bridge or secure group).	[ ]		
Affected systems, accounts and data listed. Unknowns listed.	[ ]		
Evidence preserved before any change: logs saved, images taken where needed.	[ ]		
Containment actions approved and recorded.	[ ]		
Legal and privacy lead told. Notice clocks started and times recorded.	[ ]		
Insurer and outside responders told, if the policy or plan requires it.	[ ]		
First message to staff approved by the communications lead.	[ ]		
Next update time set and announced.	[ ]		
Handover note written if the shift changes.	[ ]		

Form A: incident log

One row per entry. Never edit a row; add a new row to correct it.

No.	Date and time (zone)	Recorded by	What was observed or done	System or account	Evidence id	Decision and approver
1	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
2	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
3	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Form B: timeline

Fill in as facts are confirmed. Mark estimates with "est.".

Event	Date and time (zone)	Source of the time
First malicious activity	[ ]	[ ]
Detected	[ ]	[ ]
Reported	[ ]	[ ]
Declared	[ ]	[ ]
Contained	[ ]	[ ]
Notice clock started (one row per rule)	[ ]	[ ]

Event	Date and time (zone)	Source of the time
Notices sent (one row per recipient)	[ ]	[ ]
Recovery started	[ ]	[ ]
Recovery declared complete	[ ]	[ ]
Review held	[ ]	[ ]

Form C: handover note

Write this at every change of shift, in under one page.

- Current status and severity.
- Actions open, with owners.
- Decisions waiting, and who must make them.
- People on shift and how to reach them.
- Next update time and audience.
- Where the log and evidence are.

Form D: closing report outline

The incident lead completes this before the review meeting.

1. Summary in five sentences.
2. Timeline (Form B).
3. Cause and how it was found.
4. Impact: systems, people, data, money, hours.
5. Notices sent, to whom and when.
6. What worked and what did not.
7. Actions: owner, due date, status.
8. Changes made to this plan.