



SECURITY & RESILIENCE

Incident response starter playbook

Roles, decisions and operating records

Prepare a coordinated response to a security incident, from the first report through containment, recovery, communication and improvement.

THE WORK

Set the response authority, confirm usable contact routes and rehearse the decisions needed when a service or account may be compromised.

THE RESULT

A response team that knows who leads, what to record, how to escalate and what evidence supports a return to normal operation.

INSIDE THIS GUIDE

02 Preparation and roles

04 Contain and preserve

06 Review and rehearse

03 Report and assess

05 Communicate and recover

07–08 Response records

01 / BEFORE AN INCIDENT

Preparation and response roles

Agree authority and contact routes before an incident makes normal systems or key people unavailable.

Assign a lead and a deputy

The incident lead coordinates decisions, maintains the current priorities and confirms who owns each action. Name a deputy with enough authority to act if the lead is unavailable. Keep the role separate from the person doing every technical task.

Define who can declare an incident, isolate a service, suspend an account, authorise urgent spending and accept the operational impact of containment. Technical responders need a clear route to these decisions.

Keep a usable response workspace

Choose a controlled location for the incident record and evidence register. Set access to the people who need it and keep a way to communicate if ordinary identity, email or chat cannot be trusted.

Store the contact directory and essential recovery information so they can be reached during an outage. Verify access from an approved alternative route. Avoid placing credentials in this playbook or in a broadly shared incident document.

Connect technical and business owners

The technical lead assesses affected systems and coordinates containment and recovery. The service owner explains the business consequence and verifies restored operation. The communications owner prepares consistent updates. A record keeper maintains the timeline and decision log.

Identify specialist support, key suppliers and the appropriate legal or privacy contact. Confirm contract and insurance notification routes where relevant to the organisation. Do not wait for a complete investigation before involving the people needed to make time-sensitive decisions.

Define service priorities

Identify the services whose loss would create the greatest operational consequence and the dependencies needed to restore them. Record recovery requirements, critical suppliers and who accepts a temporary manual process.

Review the plan after material changes in systems, people or suppliers. A directory that still names a former employee creates delay precisely when the team needs a reliable handoff.

02 / ESTABLISH THE FACTS

Initial report and incident assessment

A credible report should enter a coordinated process even when its full scope is unknown.

01

Receive

Capture the observation and contact route.

02

Assign

Name the lead and affected service owner.

03

Assess

Separate confirmed facts from unknowns.

04

Act

Set containment priorities and the next update.

Capture enough to begin

Record when the issue was observed, who reported it, the affected account or service and the visible behaviour. Include actions already taken. Preserve relevant messages, identifiers and screenshots in the approved evidence location.

Ask the reporter to avoid further interaction with suspicious content or a potentially compromised account. Give a clear route for further updates. Technical investigation should be directed by the response lead and performed by people with appropriate access and capability.

Assess consequence and uncertainty

Determine which services, accounts and information may be affected; whether the activity appears ongoing; and whether the organisation can still operate safely. Treat evidence of privileged access, broad service disruption or sensitive information exposure as a reason for prompt escalation.

Record what is confirmed, what is suspected and what remains unknown. Assign the next investigation needed to reduce uncertainty. Do not wait for perfect attribution or a complete cause analysis before addressing an immediate route to harm.

First coordination decision

The lead records the incident scope as currently understood, immediate priorities, action owners, communication route and next review time. Update that assessment when new evidence changes the consequence.

03 / CONTROL THE INCIDENT

Containment and evidence handling

Containment should reduce ongoing harm while preserving the information needed for a reliable investigation and recovery.

Choose a proportionate containment action

Technical responders should identify the affected access or system boundary and propose an action: restrict an account, revoke sessions, isolate a device, disable an exposed route or suspend a service. Record the intended effect and expected business impact.

Coordinate changes so one action does not undermine another. A password reset may be insufficient if an attacker retains active sessions, tokens or another account. Verify the relevant access has actually been removed.

Maintain an evidence register

Give each evidence item an identifier and record its source, collection time and time zone, collector, method and storage location. Record transfers and access where required. Use integrity checks such as hashes for exported files when appropriate.

Keep originals protected and use controlled copies for analysis. Evidence may contain personal, confidential or legally sensitive information; access should follow its sensitivity and the investigation's purpose.

Preserve evidence before routine cleanup

Identify logs, messages, system state and records that may be overwritten or expire. Qualified responders should preserve volatile evidence where appropriate before making changes that destroy it.

Avoid indiscriminate deletion, rebuilding or power cycling simply to make an alert disappear. The technical lead should weigh immediate containment against evidence loss and use the appropriate specialist support for the situation.

Keep an action timeline

Record the action, authorising person, operator, time and observed result. Distinguish an action proposed from one completed. Include unsuccessful actions because they affect later decisions.

Use a consistent time reference and preserve the original timestamp when systems differ. A clear timeline helps responders distinguish attacker activity, ordinary use and changes made during response.

04 / RESTORE CONTROLLED OPERATION

Communication and recovery decisions

Communicate verified facts and restore the service through an explicit acceptance decision.

Maintain one approved account of the incident

Give staff and affected service owners the information they need to act: what is unavailable, what they should do, which route provides help and when to expect the next update. State uncertainty plainly.

The communications owner should coordinate external statements with the incident lead and relevant business, legal or privacy owners. Assess contractual and regulatory notification duties for the actual facts and jurisdictions involved. Record the applicable reporting deadlines and the responsible owner.

Validate the whole service

Test authentication, permissions, data integrity, background processing and critical integrations. Ask the service owner to complete the essential business task. Check customer-facing status and internal support instructions.

Reconnect or expand access in controlled stages where practical. Maintain monitoring appropriate to the incident and assign responsibility for unexpected behaviour after restoration.

Establish a recovery condition

Before restoration, confirm that the team understands and has addressed the access or weakness that enabled the incident sufficiently for the planned recovery. Verify the recovery environment, credentials, software and data are appropriate for use.

Choose a known suitable recovery point and record any expected data loss or reconciliation work. Restoring an old copy without understanding its state can reintroduce the problem or create an inconsistent service.

Record acceptance and remaining risk

The service owner and incident lead should record the accepted operating state, outstanding limitations and follow-up owners. Identify any temporary controls and when they will be reviewed.

Keep the incident open until required reconciliation and communication decisions have owners, even if the core service is available. Availability alone does not establish that all consequences have been resolved.

05 / IMPROVEMENT

Post-incident review and rehearsal

Use the response record to improve the operating system that produced the outcome.

Reconstruct the sequence

Review how the incident began, how it was detected, when ownership was established and which decisions changed the outcome. Separate verified causes from unresolved hypotheses. Examine why controls failed or why useful information was not available.

Include the people who reported, operated and communicated the incident. Focus on conditions and decisions that can be improved, including unclear authority, inaccessible contacts, weak monitoring and recovery dependencies.

Rehearse a realistic decision sequence

Select a relevant situation such as an unavailable identity service, compromised supplier account or lost device. Walk the team through reporting, declaration, containment authority, evidence handling, communication and restoration.

Ask participants to locate the actual directory and recovery information. Introduce the absence of a primary contact or a failed communication channel to verify the deputy and alternative route. A discussion should reveal what the team can actually do.

Assign specific corrective work

Convert findings into actions with an owner, expected change and verification condition. Prioritise the route that enabled harm and the gaps that slowed detection, containment or recovery.

Check completion against evidence. A revised document needs an operating test when the problem was a failed handoff or unusable recovery route. Keep accepted residual risks visible with a review trigger.

Update and retest the weak steps

Record the decisions that could not be made, missing information and unclear responsibilities. Correct those gaps before repeating the affected portion of the rehearsal.

Keep the playbook concise and current. Its purpose is to help people coordinate under pressure, with deeper technical procedures available to the responders who need them.

Response roles and escalation directory

Complete this directory before an incident. Use approved contact routes and verify that the alternative does not depend on the affected service. Keep credentials elsewhere.

Incident coordination

Incident lead and primary contact

Deputy and alternative contact

Declaration and urgent-action authority

Controlled record and communication route

Technical response

Technical lead and deputy

Critical supplier escalation route

Specialist response contact

Recovery procedure location and owner

Business and communication

Service owner and acceptance authority

Communications owner and deputy

Legal, privacy and contractual contacts

External-notification decision authority

Readiness review

Critical services and response priorities

Approved alternative operating route

Last contact check and rehearsal result

Plan owner and next review trigger

07 / ACTIVE RECORD

Incident coordination record

Use a controlled copy for each incident. Record facts and decisions here; maintain detailed evidence and technical logs in their approved locations.

Incident identifier and lead

Opened at and time zone

Confirmed facts, affected service and current impact

Unresolved questions and investigation owner

Priority actions, authority, owner and result

Include the time of each action and distinguish planned from completed work.

Next update and communication owner

Recovery or closure acceptance

Continue the timeline in the controlled incident record when more space is needed. Preserve this record with its evidence identifiers.