Third-party and supplier incident playbook

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

When to use this playbook

Use this playbook when a supplier tells you it has been compromised, when a supplier's product or update is malicious, or when a supplier holding your data may have lost control of it.

Before you start: prerequisites

Complete these before an incident, as part of planning.

- Each critical supplier is on the list in section 12 with an incident contact and a contractual notice time.
- Contracts say what the supplier must tell you, how fast, and what it may do on your behalf.
- You know what data and access each supplier has.
- You have an exercise scenario that includes a supplier failure.

Workflow

Work in this order. Record each step and its time in the incident log.

1. Get the facts from the supplier: what happened, when, what of yours is affected, and what it has done.
2. Check your own logs for activity linked to the supplier: connections, API calls, accounts and updates.
3. Contain: suspend the supplier's access, rotate shared secrets and credentials, and block affected components.
4. Assess your exposure: data held by the supplier, access it had to your systems, and customers who depend on it.
5. Decide who must be told. A supplier that is a processor must tell you without undue delay under GDPR Article 33(2); a business associate must tell the covered entity under 45 CFR 164.410.
6. Agree a shared communications line with the supplier.
7. Review the contract and the supplier's assurance after the incident.

Decision points

Stop at each of these and record the decision, the decider and the time.

Decision	Who decides	Information needed
Suspend the supplier's access?	Technical lead, executive sponsor	Risk to your systems versus the business use
Are you the controller or covered entity with a notice duty?	Privacy lead, legal	Contract role, data involved
Switch suppliers?	Executive sponsor	Alternatives, time to switch

Notices to check

Open section 10 of the plan and confirm whether any of these start a notice clock.

- If you are the controller or covered entity, your own clock may have started when the supplier told you, or earlier if you would have known with reasonable diligence.
- Check customer contracts: your customers may expect notice because of your supplier's incident.

Exit criteria and follow-up

Close the playbook only when all of these are true.

- Supplier access restored on agreed terms or ended.
- Shared secrets rotated.
- Contract and assurance updated.