Insider 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 an employee, contractor or other trusted person is suspected of misusing access, whether on purpose or by mistake.

Before you start: prerequisites

Complete these before an incident, as part of planning.

- Human resources and legal have agreed in advance how an employee case is handled.
- Access to sensitive systems is logged and reviewable.
- A written policy tells staff what is acceptable and what is monitored, as the law in your location allows.
- Responders know who may disable a person's access, and on whose authority.

Workflow

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

1. Receive the concern and record it. Limit who knows to the people in the plan.
2. Involve human resources and legal before any action against a person.
3. Preserve evidence quietly: logs, mailbox, file access, device images where counsel agrees.
4. Assess against behavior and facts, not assumptions. CISA describes the steps as define, detect and identify, assess, and manage.
5. Contain access in a way the legal team has agreed, for example disabling accounts at the time of an interview.
6. Recover assets: devices, keys, tokens and data copies.
7. Decide actions with human resources and legal, and record them.

Decision points

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

Decision	Who decides	Information needed
Is the act intentional or accidental?	Human resources, legal	Facts, intent indicators, history
When to remove access?	Incident lead, human resources	Risk of further harm versus risk to evidence
Involve law enforcement?	Legal counsel, executive sponsor	Nature of the act, data involved

Notices to check

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

- If personal data left the organization, assess it under the data breach plan.

- Employment law may limit what can be monitored and what can be said.

Exit criteria and follow-up

Close the playbook only when all of these are true.

- Access removed and assets recovered.
- Evidence stored under legal direction.
- Controls changed to reduce the chance of a repeat.