

Homework — Tabletop Exercise

~35 minutes · one scenario

This is a tabletop exercise. You are the on-call security lead. A scenario arrives in your DMs. Your job is to write the first-hour response plan — the document you would actually follow if this were real right now, not the one you would write for a compliance auditor.

Do the exercise before you open [answer.html](#). Time yourself. If your plan does not fit on one screen and you cannot execute the first three steps from memory, it is not a response plan yet.

The scenario

Tuesday 15:42. A mid-level engineer DMs you:

"I think I just pasted a production DB connection string including the password into my personal ChatGPT account while debugging a migration. What do I do?"

That is everything you know. The engineer is online and waiting for an answer. Write your first-hour response plan.

Required deliverables

1. **Containment steps with timestamps.** What do you do, and the engineer do, between T+0 and roughly T+10? Be specific about the order. Include the evidence-capture actions.
2. **Rotation list in priority order.** List every credential category you would rotate, in the order you would rotate it. For each, name the system and the owning team if relevant. Assume the chat session contained more than just the one connection string — the blast radius is the whole session.

3. **Notification list.** Who do you notify, in what order, and within what window?
For each entry say what you tell them in one sentence. Flag which notifications are conditional (for example, "only if PII reachable").
4. **Questions you need the engineer to answer right now.** Write the list of questions you would send back in your next message. These are the facts your plan depends on, and you do not have them yet.
5. **What you tell the engineer to do while you work.** A short, numbered instruction list the engineer can follow on their side in parallel with your rotation work. It should contain at least the evidence-capture and "do not" instructions, plus a clear communication channel.

Constraints

- You do not yet know which database, which environment, or whether the account had chat history enabled. Your plan has to be robust to the worst case on each.
- The engineer is on a personal device at home. There is no corp MDM coverage on that machine.
- Assume you have admin access (or one ping away) to your cloud IAM, your DB consoles, and your secret manager.
- Do not assume the provider deletion request will work. Include it, but do not let the rest of the plan depend on it.

✓ **Self-check: your plan (a) contains explicit evidence-capture instructions before any rotation, (b) tells the engineer in writing not to delete the chat, (c) rotates more than just the DB password, (d) has at least one notification with a time window attached, (e) includes a postmortem owner assignment in the first hour, and (f) treats the provider deletion request as best-effort, not as the primary remediation.**