Cloud account compromise 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 cloud identity, such as a user, administrator, service account or application, is used by someone other than its owner.

Before you start: prerequisites

Complete these before an incident, as part of planning.

- Sign-in and audit logs are on and retained in the cloud tenant.
- The accounts that can grant application consent are known and limited.
- Two-step sign-in is required, with phishing-resistant methods for administrators.
- A break-glass administrator account exists and is stored securely.

Workflow

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

1. Identify the account, the time window and the indicators: unusual sign-ins, impossible travel, new devices, new mailbox rules, new application consents.
2. Contain: revoke sessions and tokens, reset the password and require a fresh two-step enrollment.
3. Review application consents granted by the user or tenant-wide, and remove any suspicious application. Check permissions such as read and send mail.
4. Rotate administrator passwords, private keys and service account secrets where compromise is suspected.
5. Review what the account could reach and what it did: mail, files, configuration changes, new accounts.
6. Check other accounts for the same pattern, such as a password spray across many users.
7. Restore changed settings and add detections for the technique.

Decision points

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

Decision	Who decides	Information needed
Is it one account or many?	Technical lead	Sign-in patterns across accounts
Was an administrator account used?	Technical lead, executive sponsor	Role assignments, configuration changes
Was data accessed or sent out?	Privacy lead	Audit logs, downloads, forwarding

Notices to check

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

- If personal data was accessed, start the data breach plan.
- If the cloud provider is a processor for your customers, check section 12 and customer notice terms.

Exit criteria and follow-up

Close the playbook only when all of these are true.

- All sessions and tokens revoked; credentials rotated.
- No suspicious application consents remain.
- Detections are in place for the technique used.