

AI Risk and Data Boundary Card

Use the method

Set a clear boundary for one AI use before entering information or relying on its output. Use this whenever a new task, tool, or data type is introduced. The output records permitted inputs, prohibited inputs, human review, and actions the AI may perform. A completed card does not itself establish legal compliance or authorize access.

- 1. Name the use.** Define the task, intended users, selected tool, and accountable owner. Record whether the output stays internal or affects customers or other people.
- 2. Classify the information.** Identify what the task needs. Check the organization's rules and the actual approved tool configuration; do not assume all AI accounts have the same protections.
- 3. Set input boundaries.** List permitted information and information that must stay out. Use fictional or minimized data where sufficient. Removing a name alone may not make a record safe to share.
- 4. Set action boundaries.** Specify whether the AI may draft, analyze, update records, or take other actions. Keep external or consequential actions behind the required human authorization.
- 5. Set review and stop rules.** Identify who verifies the result, what evidence they inspect, and when to stop. Stop when the data permission, tool approval, or intended use is uncertain.
- 6. Review when conditions change.** Recheck the card when the tool, settings, inputs, permissions, or task changes. Record the approval source and next review date.

Worked example

Illustrative use: brainstorm a public-facing checklist using fictional examples. Permitted inputs: public service descriptions and invented business situations. Excluded inputs: passwords, private customer records, payment data, and restricted internal information.

Action boundary: draft text only. The AI may not publish, send messages, change systems, or claim approval. Reviewer: business owner, who checks facts, wording, and fit before release.

Stop trigger: a user proposes uploading a real customer file. The owner verifies the applicable rules and approved environment before changing the boundary.

Retention and access: use the organization's approved settings and record requirements. If those settings cannot be established, keep the use within the existing public and fictional input boundary.

Before you put it to work

☐ The tool and account are approved for the stated inputs.

☐ The minimum needed information is identified.

☐ Actions requiring authorization are explicit.

☐ A reviewer and a stop route are named.

If the problem keeps returning

If people keep stretching the boundary, narrow the approved use and make the excluded examples concrete. Resolve the new use separately instead of treating the old approval as blanket permission.

Connect the tools

Use AI-01 to assess the task and AI-03 to review outputs.

First use

Use the worksheet on the next page for one real task. Complete the decision fields, name the person responsible, and choose a review date. Duplicate the worksheet when you need another record.

Working worksheet

Name or team _____ Date _____

Use and accountability

Task, tool or account, users, owner, and intended output use.

Permitted inputs

Data types, approved source, minimum information needed, and approval reference.

Prohibited or restricted inputs

Information to exclude and cases needing a separate decision.

Complete and review

Action boundary

Permitted drafting or analysis; actions requiring human authorization.

Review and stop rules

Reviewer, verification checks, uncertainty handling, and stop triggers.

Configuration and review

Verified access or retention settings, evidence source, approval date, and change triggers.

Next review date _____ Approval evidence _____

Review after use

Did the actual use stay within the card? _____

Did a new data type or requested action appear? _____

Which setting or permission needs verification? _____

Who owns the next boundary review? _____

Next action _____ Owner _____ Due _____