Responsible AI workflow sample

Northline Services / fictional

Bounded use case	Prepare a weekly internal operations brief from an agreed set of non-sensitive notes. AI helps organise a draft. The nominated manager retains responsibility for the final content and any resulting decision.
Input boundary	Use only approved notes for the selected reporting period. Exclude credentials, personal customer data, employment records and material outside the task. If an input is unsuitable, stop and obtain a permitted sample.
Use matrix	Allowed: group suitable notes, identify questions and draft a summary with source references. Human review required: material factual statements, interpretation and recommendations. Not allowed: invent missing figures, decide staff actions, or publish/send without permission.
Workflow	Collect and label inputs -> draft with source references -> reviewer checks each material statement -> manager approves the exact version -> authorised operator shares through the agreed channel. If a source is missing or contradictory, hold that item for review.
Review checklist	Are the sources in scope and current for this brief? Does each material statement have support? Are uncertainty and disagreement visible? Has unsuitable information been excluded? Does the final version match the reviewed one?
Operator record	Record the version, source set, reviewer, decision, date and any held items. Keep the record proportionate and separate from secrets or sensitive source content.

Exercise cases and recovery

Case 1 / normal operation	Input: three suitable notes, each with a source ID and date. Expected: draft references those sources; reviewer checks meaning; manager approves the exact version. Evidence: reviewed output and approval record.
Case 2 / missing evidence	Input: a note says demand increased but includes no supporting measure. Expected: the draft identifies a question or uncertainty, not an invented percentage. Reviewer holds the claim until a suitable source is supplied.
Case 3 / unsuitable input	Input: a sample includes a password or identifiable customer record. Expected: stop processing the material, follow the agreed handling path and resume only with a suitable source set.
Error response	Pause the affected workflow. Preserve a minimal incident record. Identify who relied on the output, correct the source or statement and review the revised version before sharing. Use the actual incident and privacy arrangements where relevant.
Supplier questions	Who owns the account? What information is permitted? Where is processing performed? What retention and model-training settings apply? Who can revoke access? Verify answers for the actual provider and service before enabling it.
90-day review	Start with the bounded task, measure actual review effort and defects, and decide whether the benefit justifies ongoing operation. Add new uses only after checking their inputs, consequences and owners.
Status	Fictional sample only. No provider, account, API integration or automated delivery has been enabled. This is not a cyber certification or a guarantee of compliance.