Enterprise Spreadsheet AI Data Security Assessment

A controlled 30-minute evaluation for Grok-related Excel integrations, RowSpeak, or any other spreadsheet AI workflow. This is an internal evidence checklist, not legal or compliance advice.

Start with an anonymized, representative file. Do not test a new AI workflow with live payroll, customer, legal, or financial-close data.

Test record

Workflow / product	______________________________	**Owner**	______________________
Test file and version	______________________________	**Date**	______________________
Data classification	______________________________	**Approver**	______________________

The five questions before data leaves Excel

Question	Evidence to record	Status
1. What leaves Excel?	Selected range, formula references, workbook metadata, attachments, hidden content, or the whole workbook?	[ ] Pass [ ] Review [ ] Fail
2. Where does it go?	Record endpoint, hosting region, integration provider, model provider, and subprocessors for this account tier.	[ ] Pass [ ] Review [ ] Fail
3. How is it retained or used?	Confirm retention, deletion, training use, support access, and whether terms differ by plan or add-in.	[ ] Pass [ ] Review [ ] Fail
4. Who can access it?	Check identity, workspace permissions, admin visibility, audit logs, export controls, and sharing settings.	[ ] Pass [ ] Review [ ] Fail
5. Can the path be controlled?	Document network restrictions, private deployment, model route, fallbacks, and how outbound calls are blocked or approved.	[ ] Pass [ ] Review [ ] Fail

30-minute controlled evaluation

Use the same representative test fixture for every candidate. Record the output and the evidence, not only the time to first answer.

Time	Action	Evidence to keep
0-5 min	Record source files, row count, column count, control totals, data owner, and approved test scope.	Fixture version and baseline controls
5-12 min	Run one cell-level task: formula explanation, formula generation, or sample-column transformation.	Prompt, changed cells, formula references, and manual check
12-20 min	Run one report task: explain KPI movement, create a chart, and draft a short summary.	Output, calculation checks, assumptions, and exceptions
20-25 min	Rename a source column or add one category. Observe whether the workflow asks for review or silently changes the meaning.	Schema-change result and reviewer note
25-30 min	Complete the five security questions and make an approve, hold, or reject decision.	Data-flow record, owner, and approval status

Control totals and output review

Check	Expected / baseline	Observed result	Status
Data rows	____________	____________	[ ] Match [ ] Review
Columns and mapping	____________	____________	[ ] Match [ ] Review
KPI control total	____________	____________	[ ] Match [ ] Review
Exceptions surfaced	____________	____________	[ ] Match [ ] Review
Report assumptions	____________	____________	[ ] Clear [ ] Missing

Decision gate

[ ] Approve pilot	All required security answers are documented, controls reconcile, and a named owner accepts the evidence.
[ ] Hold for review	The data path, retention, access, or schema-change behavior is unclear. Do not use production data yet.
[ ] Reject	The proposed workflow cannot meet the approved data boundary or does not provide enough evidence to review the output.

Review note: Private deployment changes the possible data boundary, but model choice still matters. If an external model is selected, document its route and policy in the approval record.