

Appendix F: AI Vendor Evaluation Questionnaire

Use this questionnaire before any AI tool, feature, or model service touches company data above Public, and again at each renewal (Chapters 10, 21, and 25). It expands Owen’s five vendor questions from Chapter 10 into a full review; send it to the vendor, ask for dated, written answers, and record the evidence. A vague answer is an answer, and it is not a pass.

How to use it

Fill in the tool, the vendor, the reviewer, and the date at the top of your copy. For each question, write the vendor’s answer, the evidence (the document, section, and date, or the name of the person who answered in writing), and mark Pass as yes, no, or condition. A condition is something that must be fixed before live use, with an owner and a date. Any “no” in section 1 or 2 stops the review for Confidential or Restricted data.

1. Training and data use

Table 1: Training and Data Use. Pass requires 1.1 to be “no” and 1.2 to be “yes” for Confidential data.

#	Question	Answer	Evidence (document, date)	Pass?
1.1	Do you train or improve any model on our inputs, outputs, or files?			
1.2	Is training use excluded in writing in our contract or plan terms, not only in a settings screen?			
1.3	If an opt-out is needed, is it on by default for our whole account, and who can switch it back?			
1.4	Do your staff ever read our data, and under what conditions?			
1.5	Can your terms on data use change without notice to us?			

2. Retention, deletion, and where data goes

Table 2: Retention, Deletion, and Where Data Goes.

#	Question	Answer	Evidence (document, date)	Pass?
2.1	How long do you keep inputs, outputs, files, transcripts, and logs, counting every copy and backup?			
2.2	Can we set our own retention period?			
2.3	Can we delete our data on request, and will you confirm deletion in writing?			
2.4	Which subprocessors (any third party processing our data for you, such as the model provider) receive our data, and will you tell us before adding one?			
2.5	In which countries is our data stored and processed?			
2.6	Do you keep data for abuse monitoring, and for how long?			

3. Sign-in, access, and permissions

Table 3: Sign-in, Access, and Permissions.

#	Question	Answer	Evidence (document, date)	Pass?
3.1	Does it support our company sign-in, with multi-factor authentication?			

#	Question	Answer	Evidence (document, date)	Pass?
3.2	Does it support single sign-on, so disabling one account removes a leaver?			
3.3	Can an administrator see and remove every user, connection, and key?			
3.4	For a workflow, can it run under a service account with only the permissions the task needs, with read and write set separately?			
3.5	If it searches company documents, does it respect our existing access rules, so no one sees what they could not open themselves?			
3.6	Which features or connections are switched on by default, and can we switch each off?			

4. Logging, control, and safety

Table 4: Logging, Control, and Safety.

#	Question	Answer	Evidence (document, date)	Pass?
4.1	Can we get usage logs showing who did what, when?			
4.2	For workflows, can we log input, output, approver, and action?			

#	Question	Answer	Evidence (document, date)	Pass?
4.3	Can we switch the tool or a single workflow off at once?			
4.4	What can the tool do without a person approving it (send, change, delete, pay)? Can we limit that?			
4.5	How do you defend against instructions hidden in content the tool reads? Will you let us run our own hostile-input tests (Checklist 10.1)?			
4.6	Can answers show the sources they came from?			
4.7	How will you tell us about a security incident affecting our data, and how fast?			

5. Cost, change, and exit

Table 5: Cost, Change, and Exit.

#	Question	Answer	Evidence (document, date)	Pass?
5.1	What does it cost per seat, plus any per-task or usage charges that grow with volume?			
5.2	How much notice do you give before price rises or plan changes?			
5.3	Will you tell us before changing the underlying model?			

#	Question	Answer	Evidence (document, date)	Pass?
5.4	How do we export our data, settings, and history, and in what format?			
5.5	Will you export and delete a non-sensitive test sample with us before we sign (Chapter 25)?			
5.6	What are the term, auto-renewal, and notice period for cancelling?			

Decision record

Table 6: Vendor Review Decision Record. File it with your approved tool list (Chapter 10, control 1).

Item	Entry
Tool and vendor	
Use approved	
Highest data class approved (Public, Internal, Confidential, or Restricted)	
Features kept switched off	
Conditions to clear before live use, with owner and date	
Owner and second person who can switch it off	
Reviewer, approver, and date	
Next review date (at renewal, or within 12 months)	

Answers that touch contracts, privacy law, or regulated data go to your legal adviser; this questionnaire is operational guidance, not legal advice. Vendor terms change, so date every review and repeat it at renewal.