AI Tool Due Diligence Checklist

Use this checklist before approving any AI tool or pilot to identify material confidentiality, privilege, and data security risks; and confirm they're contractually and technically controlled before client data is used.

Data Use & Model Behavior

☐ Does the vendor train or fine-tune on customer data by default?

☐ Can you contractually prohibit any training or product-improvement use of your data?

☐ Does the system use human review for prompts/outputs (e.g. for quality improvement)? Can you opt out?

☐ Does the tool have "memory," shared workspaces, or features that could create cross-matter leakage?

Retention, Storage, And Access

☐ What is retained: prompts, files, outputs, embeddings, logs?

☐ Can you disable history or set short retention windows?

☐ Who can access stored data at the vendor (support, engineers)? Is access least-privilege and logged?

☐ Can you export usage and access logs without exporting or duplicating substantive prompt or client content?

Security Controls

☐ Is SSO integrated and MFA enforced for all users, including administrators?

☐ Does the platform support granular RBAC with restricted and auditable administrative access?

☐ Is tenant isolation documented, with logical (and where applicable physical) segregation from other customers?

☐ Is data encrypted in transit and at rest using documented, industry-standard controls?

☐ Does the vendor conduct regular vulnerability management and third-party penetration testing, with documentation available?

Subprocessors And Residency

☐ Where does the data live (e.g., in the US, EU, or both)? Can you choose residency?

☐ Who are the subprocessors (e.g., hosting, analytics, model providers)?

☐ How are subprocessor changes communicated to users?

Incident Response

☐ What is the incident response process and breach notification timeline?

☐ Are there clear escalation contacts and procedures?

Exit / Termination

☐ Can you verify deletion of your data on contract termination (including retained content and backups where applicable)?

☐ Can you retrieve your data in a usable format before offboarding?