Making AI Easy

CREW | Follow-Up Reference | 16 October 2026

Anthony Peters, IT Systems Manager, BranchPattern

TWO DIFFERENT QUESTIONS

Both matter. For different reasons.

SECURITY

Who can access the data, and where can it go?

Account and contract
Permissions and connectors
Retention and sharing

Lease example: Confidential lease in an unapproved account.

SAFETY

Is this output reliable enough for the intended use?

Evidence and completeness
Professional review
Authority to act

Lease example: AI omits a renewal condition.

A secure tool can still be wrong. A correct answer can still disclose data improperly.

NEW WORDS FOR NEW TECHNOLOGY

Token — Parts of text AI reads and writes. Limits and costs are counted in tokens, not words.

Model — Trained software that predicts likely next words; not itself a search engine.

Prompt — Your request plus the context you provide.

Grounding — Connecting answers to real sources or documents for evidence.

Context window — The tokens AI can process at one time.

Hallucination — Confident but incorrect output.

Agent — AI with a goal, instructions, tools and permission to take specified steps or actions.

Tenant — Your organization's contractual and technical cloud "fenced yard," governed by controls and policies—not a guarantee that all data stays inside.

Permissions — Existing access AI can use to surface content, including files you have forgotten.

Training & inference — Training builds a model; inference uses it. Covered business Copilot prompts and responses are not used to train foundation models; verify the exact service and contract.

Prompt injection — Malicious or hidden instructions in a file, email or web page that try to redirect AI actions.

Instructions — Standing guidance across AI or agent interactions.

THE FENCED YARD IS NOT A FREE PASS

An approved work account is not permission to upload everything. Keep client or firm data out of unapproved public tools. Check the exact service and connection: consumer and business terms differ; web search and connected agents may handle data differently.

Review broad sharing, separate client/deal files, and use least-privilege connectors.

BEFORE YOU USE OR ACT

Human accountability stays with you.

01 Approved tool / work account

02 Permitted data / access

03 Ground; check evidence and completeness

04 Professional review; human approval before consequential action

Source: CREW Presentation - Making AI Easy.pptx, slides 5–11