Prompt & Context Engineering — Manager Cheat Sheet

Prompt Engineering: steer the model. Keep it structured, testable, and governed.
Context Engineering: ground the model with trusted data at inference.

Enterprise Prompt Patterns

- Role + Objective: define who the model is and the measurable outcome.
- Format First: require JSON/YAML tables; reject free text.
- Guardrails: cite sources, note uncertainty, escalate when low confidence.
- Few-shot: 1–2 canonical examples, no private data.

Context Lifecycle

- Ingest: policies, KBs, tickets, logs, APIs.
- Index: vector/graph with metadata (owner, PII flags, TTL).
- Retrieve: filters (team, region), freshness SLAs.
- Cite & Store: include citations; redact PII; apply retention.

KPIs to Track

- Time saved per task
- Answer accuracy (HITL pass rate)
- Escalation rate
- Compliance violations prevented

	Prompt	Context
Purpose	Intent, role, policies, format	Facts, evidence, examples
Governance	Versioned templates, linting, A/B tests	Source of truth, freshness SLAs, PII controls
Where used	Every request	As needed via retrieval/tools (MCP)

Tip: Treat prompts and context as configurable assets, with reviews and change control just like code.