

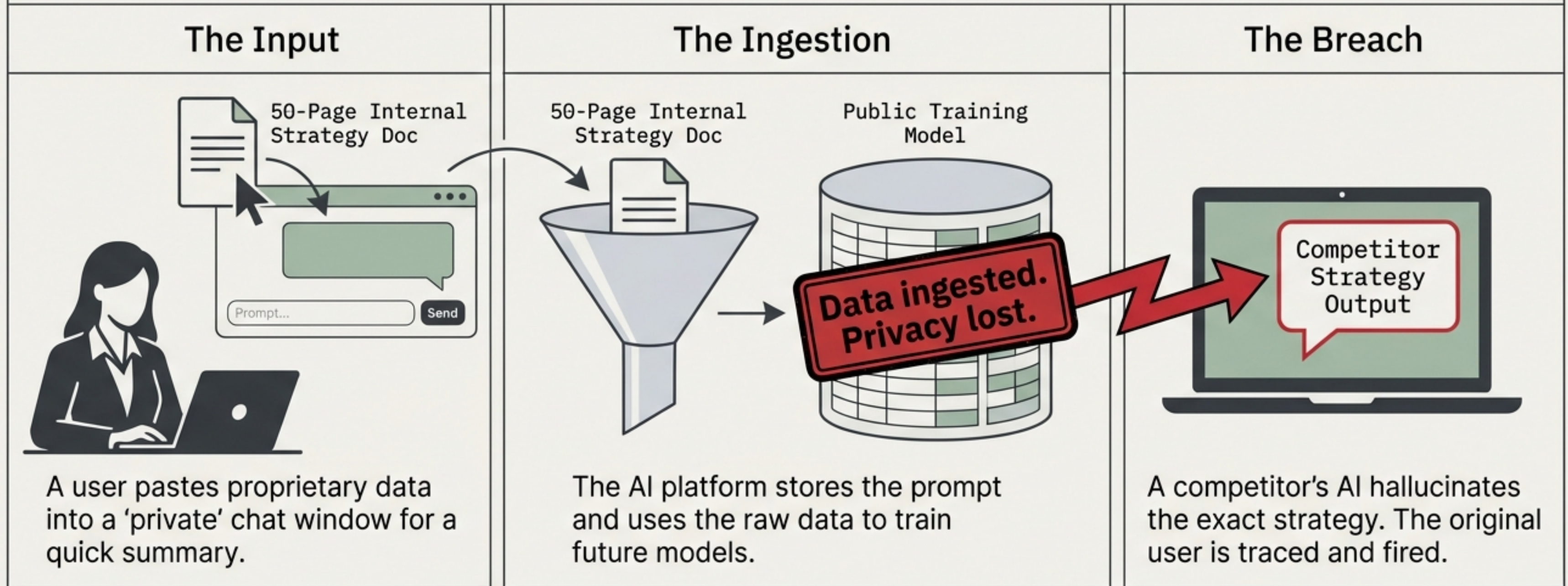
CLEARANCE: LEVEL 5
STATUS: CONFIDENTIAL

The Digital Dossier

AI Hygiene & Data Security

Operational protocols for protecting your career data, maintaining NDA compliance, and safely leveraging Generative AI.

The Invisible Breach: The AI Data Vacuum



Treat any AI chat interface like a town gossip. If you wouldn't print it on a billboard, do not paste it into the prompt box. AI is excellent at organization, but terrible at keeping secrets.

The Red Zones: Absolute Data Prohibitions

AI Hygiene:

The disciplined practice of managing AI data inputs to prevent the leakage of sensitive, confidential, or proprietary information.



Personally Identifiable Information (PII)

Specific details linking individuals to datasets. Never share SSNs, home addresses, or personal phone numbers.



Proprietary Information

Internal processes, trade secrets, or raw software code from current or former employers.

**NEVER
FEED TO
AI**



Financial & Strategic Data

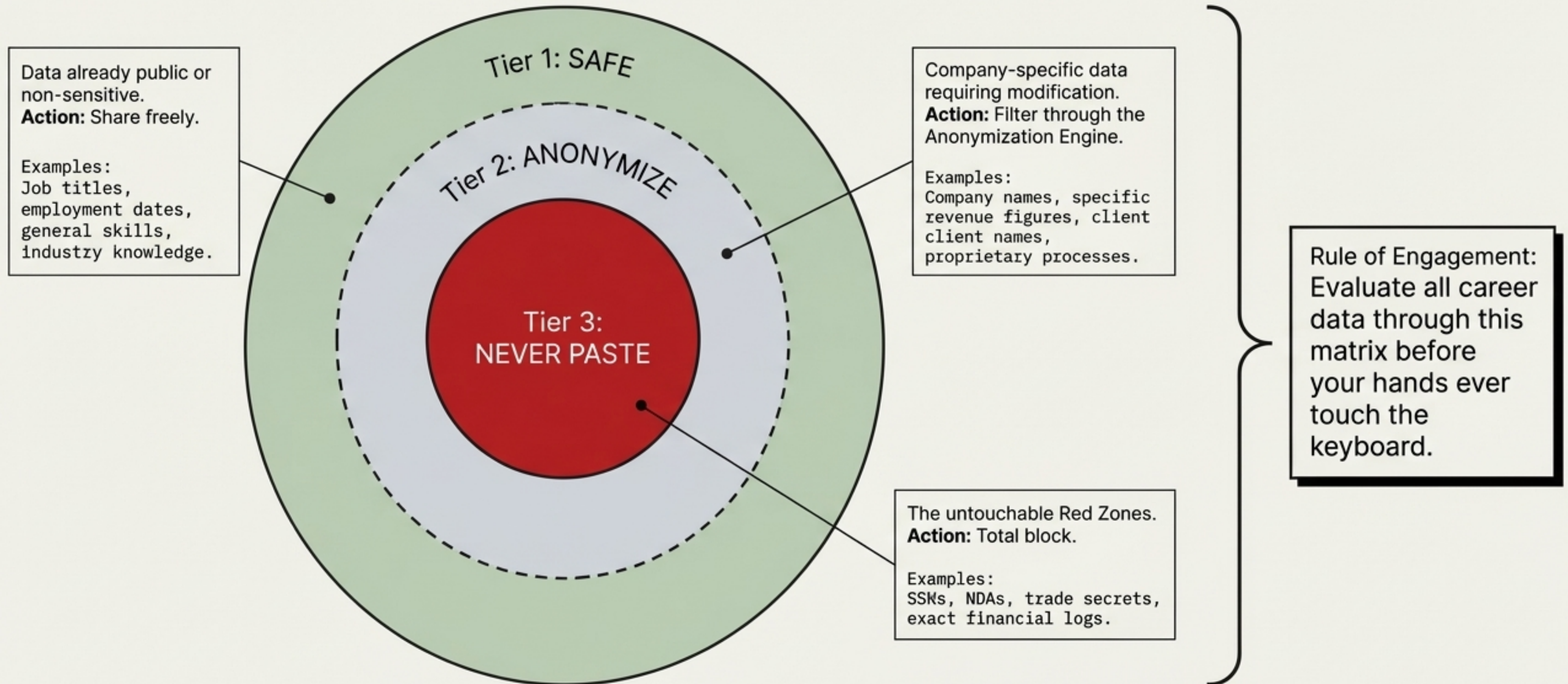
Non-public revenue figures, internal growth metrics, budget numbers, or strategic roadmaps.



Contractual Data

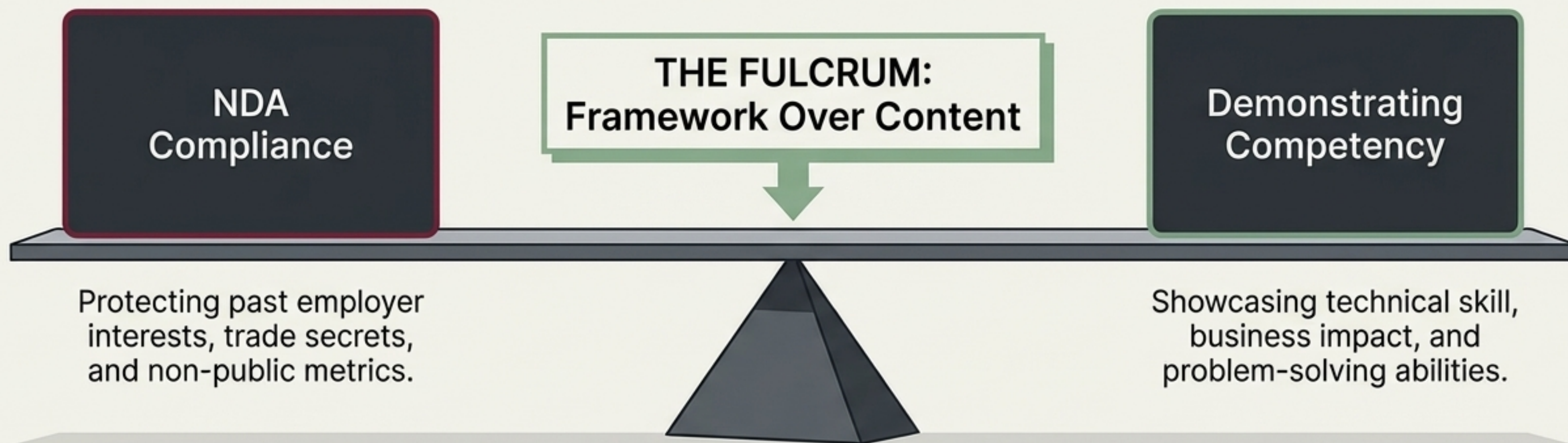
Any specific client names, project codenames, or information governed by a Non-Disclosure Agreement (NDA).

Triage Protocol: The 3-Tier Classification Model





The Case Study Balancer: Proving Value Without Leaking Secrets



The Mechanism —

Feed the AI a generalized “problem-solution” framework.

Let the AI structure the narrative flow, but keep proprietary implementation details completely out of the prompt.

The Technique —

Transform real proprietary projects into hypothetical scenarios.

Ask the AI to solve an architectural challenge conceptually, rather than auditing your actual past code.

Execution: The Prompt Transformation Matrix

The Leaky Prompt

I used the internal [SwiftPay] engine at [Chase] to reduce transaction latency for [500,000] [500,000] retail customers by [150ms].

STATUS: High Breach Risk. Contains Tier 2 & Tier 3 data.

The Clean Prompt

I optimized a [proprietary payment processing system] at a [Top-5 Global Bank], reducing transaction latency for a [large-scale retail user base] by [25%].

STATUS: Cleared. Maintains impact, protects identity.

Analysis:

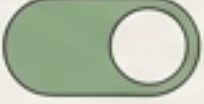
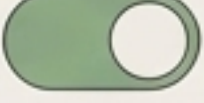
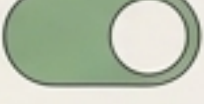
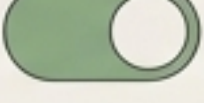
The clean prompt demonstrates specific scalability and technical skills without mentioning proprietary company names, triggering an NDA breach, or leaking raw data.



STRATEGIC RULE

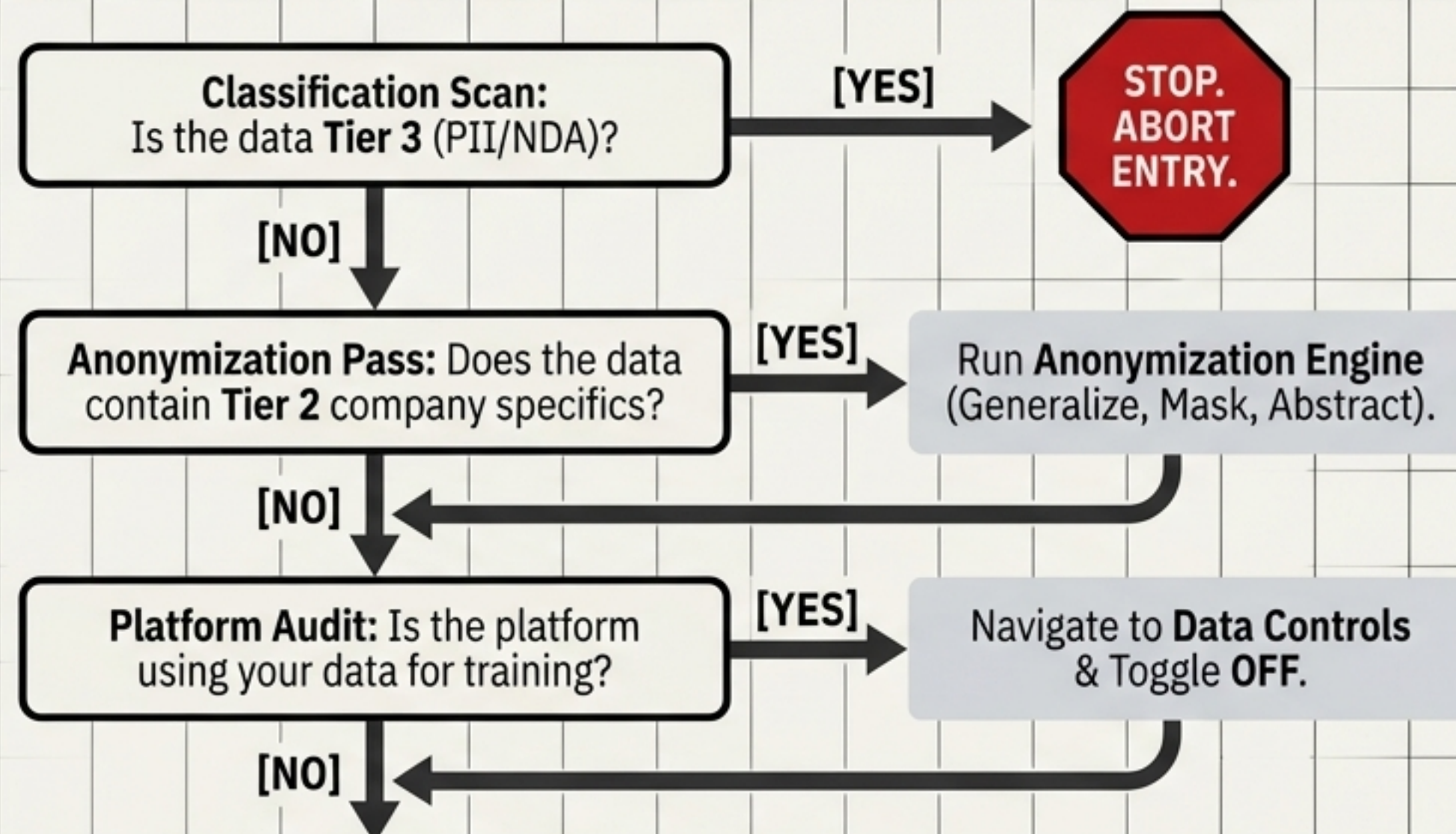
Inter: Use the Burner Profile to test prompt quality, map AI behavior, and refine outputs. Only replace burner data with real data offline in your final, localized documents.

System Diagnostics: The 5-Point Privacy Audit

	Criteria	Verification Method	Status Toggle
1.	Training Policy Review ^{Inter}	Does the ToS state they use your input to train public models? ^{Inter}	 IBM Plex Mono FAIL
2.	Opt-Out Capability	Is there a clear, accessible setting to turn off data sharing?	 PASS
3.	Data Deletion	Are there options to export and completely delete account logs?	 PASS
4.	No PII Required	Can the tool be used effectively without providing a real name/email?	 PASS
5.	Enterprise / Privacy Mode	Does the platform offer a secure, privacy-first paid tier?	 PASS
			AUDIT SCORE: 4 / 5

Diagnostic Rule: A tool must score at least a 4/5 to be cleared for job search operations. Most default consumer tiers harvest data; you must manually navigate to settings and toggle them off. (Inter)

Standard Operating Procedure: Pre-Flight Checklist



The 3 Final Tests



Public Post Test: Would this compromise you on a public forum?



Former Boss Test: Are trade secrets protected?



Outcome Check: Is the prompt still specific enough for AI to help?

> [ALL CHECKS CLEARED]
> EXECUTE PROMPT.