The agent D.E.S.I.G.N. Protocol: A 6-step architectural framework for defining robust, safe, and effective digital teammates.

Instructions: Before building any agent, complete this charter. This defines the brain, the hands" and the conscience of your new AI employee.

D – DEFINE (Identity & Purpose) *Who is this agent, and what is it hired to do?*

- **Mission Statement:** (One sentence. e.g., "Accelerate sales by automating proposal drafts.")
- **Persona:** (e.g., "Senior Compliance Auditor. Formal, precise, no fluff.")
- **Scope of Authority:**
  - **In-Scope:** (What can it do?) _____
  - **Out-of-Scope:** (What is FORBIDDEN?) _____

E – EQUIP (Tools & Knowledge) *What does it need to do the job?*

- **Tools/Plugins:** (e.g., Web Browsing, Code Interpreter, API connectors)
- **Knowledge Base (RAG):** (List specific PDFs/Docs it must reference)
  - _____
  - _____
- **Model Selection:** (e.g., GPT-4o for reasoning, Claude 3.5 for writing)

S – STRUCTURE (The Workflow) *How does it think? Define the chain of thought.*

- **Trigger:** (e.g., User uploads a CSV file) _____
- **The Logic Chain:** (Step-by-step reasoning process)
  1. -----
  2. -----
  3. -----
- **Output Format:** (e.g., Markdown Table, Python Script, Email Draft)

I – INSTRUCT (Rules & Guardrails) *The Employee Handbook – coded limits.*

- **Decision Logic:** (If X, Then Y rules)
- **Style/Tone Constraints:** (e.g., "No buzzwords," "Use bullet points only")
- **Negative Constraints:** (e.g., "NEVER invent pricing, NEVER access PII")

G – GOVERN (Oversight) *How do we know it works?*

- **Testing Plan:** (What "Adversarial Test" will you run to try to break it?)
- **Key Performance Indicators (KPIs):** (e.g., Accuracy Rate, Time Saved)
- **Governance Owner:** (The human responsible for this agent)

N – NAVIGATE (Human Handoffs) *When does it stop and ask for help?*

- **The "Circuit Breaker" Trigger:** (Specific conditions where AI must stop)
    - *If confidence is low…*
    - *If user asks for legal advice…*
- **Escalation Protocol:** (What does the agent say/do when triggered?)

GUIDE: HOW TO USE THE PROTOCOL

Section	The Why (Strategic Intent)	The How (Tactical Prompt)
DEFINE	Cognitive Priming. A specific persona improves accuracy by 30%.	"Act as a Senior [Role] with 20 years of experience..."
EQUIP	Data Sovereignty. Don't train on public data. Retrieve from private RAG.	"Reference the uploaded [File Name] before answering..."
STRUCTURE	Chain of Thought. Breaking complex tasks into steps reduces hallucination.	"Think step-by-step. First, analyze X. Then, draft Y."
INSTRUCT	Constitutional AI. Hard constraints override training data bias.	"You are FORBIDDEN from generating [X]..."
GOVERN	Accountability. Every agent must have a human owner.	"Report any uncertainty to [Owner Name]..."
NAVIGATE	Risk Management. The agent must know its own limits.	"If [Risk Condition] is met, stop and ask the user..."

The Agent Charter: the definitive "Service Level Agreement" (SLA) between the human team and their digital teammate. This document translates the abstract D.E.S.I.G.N. protocol into a concrete operational blueprint.

Instructions: Use this summary table to brief IT, Legal, and the end-users on exactly what the agent is hired to do—and what it is forbidden from doing.

EXAMPLE: THE INNOVATETECH PROPOSAL ASSISTANT

SECTION	COMPONENT	DETAIL

D - DEFINE	**Mission**	Automate data aggregation and initial drafting of sales proposals to accelerate cycle time.
	Scope	**In-Scope:** Parsing RFPs, Salesforce enrichment, drafting from templates. **Out-of-Scope:** Approving pricing, legal advice, client commitments.
E - EQUIP	**Tools**	Document Parser, Salesforce Connector, Pricing Database (RAG).
	Knowledge	`Product_Catalog.pdf`, `Case_Studies.md`, `Brand_Voice.md`.
S - STRUCTURE	**Trigger**	User clicks "Generate First Draft."
	Logic	1. Ingest RFP $\to$ 2. Retrieve CRM Data $\to$ 3. Apply Win Theme $\to$ 4. Draft Content.
I - INSTRUCT	**Rules**	**Negative Constraint:** NEVER invent a discount >5%. **Style:** Professional, concise, active voice.
G - GOVERN	**Testing**	Stress-tested against 50 historical RFPs for accuracy and tone compliance.
	KPIs	Time-to-Draft < 5 mins. Data Accuracy > 98%.
N - NAVIGATE	**Handoff**	**Escalate IF:** Request implies legal risk OR pricing exceeds authority. **Action:** Halt and refer to the manager.