Instructions for AI - Data Handling Protocol (Internal Support Tools)

AI Tool: Gemini-Powered Support Assistant (Internal)
Audience: L1/L2 Support Agents
Objective: Define security and privacy protocols when interacting with client data via the internal AI assistant.

Protocol: Client Ticket Summarization

The internal Support Assistant is used to quickly summarize long ticket threads, analyze log snippets, and draft resolution emails.

1. Mandatory Data Masking (CRITICAL)

When providing a client log snippet or workflow details to the AI Assistant, you **MUST** ensure the following Personal Identifiable Information (PII) and highly sensitive enterprise data points are masked or replaced with placeholders:

Data Type	Example of Masking
Client PII (User Level)	Replace real names/emails with [USER_A], [USER_B], [EMAIL_MASKED].
API Keys / Secrets	Replace with [API_KEY_MASKED]. Never input full keys.
Financial Values	Replace specific dollar amounts with [FIN_VALUE].
Private IP Addresses	Replace internal IPs with [IP_MASKED].

Rationale: This practice ensures compliance with internal Data Privacy Policy, preventing highly sensitive client data from entering the large language model's context window.

2. AI Prompting Guidelines

When asking the AI to analyze a ticket, always include the following contextual constraints:

1. **Role Definition:** Start with: "Act as a NexaCore L2 Support Specialist."
2. **Goal:** State the precise action: "Analyze the attached log and determine the most likely root cause."
3. **Output Format:** Specify the output: "Provide a 3-point bulleted summary. Do not use

external sources."

3. Verification of AI-Generated Content

- **Drafted Resolutions:** If the AI Assistant drafts a resolution or RCA for you, you **MUST** review it for technical accuracy before sending it to the client.
- **Compliance Check:** Agents are responsible for the final output. If the AI provides unmasked sensitive data, the agent must correct it and report the prompt failure to the Head of Support.