Since we are building the **Penuel Unified "Empire" portal** as a fresh React-based system rather than patching old code, we need a technical foundation that prioritizes both security and the specific "Hub-and-Spoke" architecture required for your business.

Here is the technical blueprint for the new system, incorporating the security guardrails necessary to protect your revenue and data.

---

1. The Secure Architecture (The "Empire" Portal)

The new system will replace the "Dumb Shell" HTML approach with a **Secure Component Model**.

- **Business Switcher Logic:** Instead of separate HTML files for different branches, a single React "Context" will manage whether the user sees the **Plaza** (Gold/Navy) or **Stopover** (Green/Amber) theme.
- **The Logic Hub (Weeks 4-5):** This central layer will handle all **M-Pesa Daraja** and **Airtel Money** API integrations.
- **Unified Dashboard:** A single administrative view will consolidate revenue tracking across the Hotel, Car Wash, and Supermarket.

---

2. Security Protocols & Implementation

To address your concerns about AI-generated security risks, we are implementing the following "Hard Guardrails" from the start:

A. Identity & Access (The "Front Door")

- **API Authentication:** Every request from the React frontend to your VPS will require an `x-api-key` in the request headers. This prevents unauthorized parties from fetching or tampering with your pricing data.
- **Staff Verification:** We are implementing a **"Human-in-the-Loop"** system for Milestone 2. This means digital orders must be manually "Accepted" by designated managers before they are finalized in the system.

B. Data Protection

- **Credential Masking:** Sensitive database credentials, M-Pesa Till/Paybill numbers, and Airtel Merchant IDs will **never** be hardcoded into the frontend code.

- **Environment Isolation:** All sensitive keys will be stored in server-side environment variables, ensuring they remain hidden from the public-facing portal.

---

3. Development Roadmap (6-Week Sprints)

This schedule ensures that security testing is baked into the process, not tacked on at the end.

Phase	Timeline	Security & Technical Focus
The Interface	Weeks 1–3	Deployment of SSL Security setup and VPS infrastructure.
The Logic Hub	Weeks 4–5	Integration of payment gateways and the manager-led verification system.
The Launch	Week 6	**Final Security Testing** and AI Assistant training before the "Live" switch.

---

4. Next Technical Steps

To move forward with the **Milestone 1 Kickoff**, we need to secure the infrastructure that will host these security layers.

1. **Infrastructure Setup:** Provision the high-performance VPS and register the .co.ke domain.

2. **SSL Activation:** Immediately install SSL certificates to ensure all data between the

"Empire" portal and your staff is encrypted.

3. **Data Collection:** Begin gathering high-resolution logos and service menus for the initial "Business Switcher" build.