

TradeArchitect LLC

Cybersecurity policy

1. Data Security & Encryption Policy

Objective: To ensure all sensitive financial data is unreadable to unauthorized parties.

- **Encryption at Rest:** All sensitive credentials, including Broker Access Tokens and API Keys, are encrypted before being stored in our primary database (PostgreSQL). We utilize industry-standard **AES-256 encryption**.
- **Encryption in Transit:** All communication between the Desktop Client and the Railway Backend is forced over **TLS 1.3 (SSL/HTTPS)**. No "plain text" data is ever transmitted.
- **WebSocket Security:** Real-time notifications are delivered via **Secure WebSockets (WSS)**. Every connection is authenticated using a "Ticket-based" or JWT handshake to ensure data is only routed to the verified owner of the account.

2. Infrastructure & Backend Safety (Railway)

Objective: To leverage cloud-native security features provided by our hosting provider.

- **Isolated Environments:** Our Railway backend operates in a containerized environment with a strict private networking layer. The database is not accessible from the public internet; it only accepts connections from the internal application service.
- **Zero-Persistence Strategy:** We minimize the storage of PII (Personally Identifiable Information). Our backend acts primarily as a "secure relay" between the user and their chosen brokers.

3. Authentication & Access Control

Objective: To ensure only the rightful owner can access their trading data.

- **Identity Management:** We utilize **Auth0** for identity providing, ensuring that user passwords never touch our servers.
- **OAuth 2.0 Protocol:** We follow the official OAuth 2.0 "Authorization Code" flow for all broker connections. This means your broker passwords remain between you and the broker (Alpaca, Schwab, etc.); we only receive a limited-access "token" to execute trades on your behalf.
- **State Verification:** To prevent "Man-in-the-Middle" or "Cross-Site Request Forgery" (CSRF) attacks, every authentication request includes a unique, one-time **state** GUID that is verified upon callback.

4. Privacy & Data Ethics (The "No-Sell" Pledge)

Objective: To transparently state our business model regarding user data.

- **No Sale of Data:** We do **not** sell, rent, or trade your personal information, trading history, or broker connections to any third parties, including hedge funds or data aggregators.
- **Data Minimization:** We only collect the data necessary to provide the trading architect functionality. If you disconnect a broker, all associated tokens are purged from our active records.