ZERO STATE SECURITY | PRIVACY & DATA POLICY

1. SCOPE: This policy governs the handling of all data collected during the term of the security audit. **2. DATA MINIMIZATION:** Zero State Security follows a "Zero-Persistence" philosophy. We do not download or store Client database records. Any data incidentally viewed during testing is kept only in volatile memory for the duration of the proof-of-concept. **3. ENCRYPTION & STORAGE:** All technical findings and draft reports are stored in AES-256 encrypted volumes. Communication regarding findings is conducted via secure email (**audit@zerostatesecurity.com**) or encrypted messaging. **4. NO THIRD-PARTY PROCESSING:** No Client data or vulnerability metadata is uploaded to third-party AI models, public cloud scanners, or external "Threat Intelligence" databases. All analysis is performed locally via the Patch3 Engine. **5. DATA DESTRUCTION:** 30 days after the conclusion of an engagement and final payment, Zero State Security will securely purge all technical evidence and draft documents, retaining only the final signed report for legal records.