ZERO STATE SECURITY | RULES OF ENGAGEMENT

1. AUTHORIZATION & SCOPE: Client hereby grants Zero State Security ("Consultant") explicit permission to perform offensive security testing on the IP addresses, domains, and cloud environments defined in the Statement of Work. Testing of any asset not explicitly listed is strictly prohibited. **2. REMOTE-ONLY OPERATIONS:** All testing is conducted via secure remote infrastructure. Consultant will not require physical access to Client premises. Client is responsible for ensuring that remote access points are available during the testing window. **3. THE PATCH3 FRAMEWORK:** Consultant utilizes the proprietary Patch3 Analysis Engine. While these tools are engineered for non-disruptive auditing, Client acknowledges that security testing involves sending unconventional traffic to systems which may, in rare cases, cause service instability. **4. DATA DISCOVERY PROTOCOL:** If Consultant gains access to sensitive data (PII, PHI, or Financial Records), Consultant will: (a) Cease testing on that specific vector; (b) Capture only the minimum evidence required to prove the vulnerability; (c) Notify the Client’s primary contact immediately. **5. RESTRICTED ACTIONS:** Consultant shall not perform: (a) Distributed Denial of Service (DDoS) attacks; (b) Permanent deletion of production data; (c) Intentional disruption of critical business logic unless requested for "Stress Testing" purposes.