ZERO STATE SECURITY | RULES OF ENGAGEMENT

1. AUTHORIZATION & SCOPE: For Security Audits, Client grants Zero State Security ("Consultant") explicit permission to perform offensive testing on defined assets. For KVM VPS services, the Client is granted permission to utilize ZSS infrastructure for legal, professional, and research purposes only.

2. REMOTE-ONLY OPERATIONS: All operations are conducted via secure remote infrastructure. Consultant will not require physical access to Client premises. Client is responsible for ensuring that remote access points or VPS instances remain accessible via the provided credentials.

3. THE PATCH3 FRAMEWORK: ZSS utilizes the proprietary Patch3 Analysis Engine. While engineered for non-disruptive auditing, Client acknowledges that security testing involves sending unconventional traffic which may, in rare cases, cause service instability. ZSS is not liable for incidental downtime during authorized testing.

4. DATA DISCOVERY & PRIVACY PROTOCOL: If Consultant gains access to sensitive data during an audit, Consultant will: (a) Cease testing on that vector; (b) Capture minimum evidence; (c) Notify Client immediately. For VPS services, ZSS does not access Client data but will comply with lawful requests for information from competent legal authorities if presented with a valid warrant.

5. INFRASTRUCTURE ANTI-ABUSE POLICY (VPS ONLY): Clients utilizing KVM VPS infrastructure are strictly prohibited from:

- (a) Performing unauthorized DDoS or DoS attacks against third parties;
- (b) Hosting or distributing Malware, Ransomware, or illegal materials;
- (c) Engaging in "IP Spoofing" or activities that trigger "Abuse Reports" from upstream providers;
- (d) Any activity that results in the "Blacklisting" of ZSS-owned IP space.

6. RESTRICTED ACTIONS & DISRUPTION: Consultant shall not perform intentional disruption of production data during audits. Conversely, for VPS services, **ZSS reserves the right to suspend or terminate any instance immediately and without refund** if the instance is found to be in violation of Section 5 or is causing a "Critical Threat" to the ZSS network backbone.