Kravitz Group Holdings, LLC.,
Physical Security, Cybersecurity Policies & Procedures
(As required by 21VAC5-80-260 (A))

How Kravitz Group Holdings Protects Your Privacy
At Kravitz Group Holdings (KGH), we recognize the trust you place in us when you disclose personal information. Maintaining that trust by ensuring that your information is secure is core to our business. Our dedicated Registered Representative and/or Chief Compliance Officer is committed to the privacy and protection of your personal information entrusted to us.

From technological safeguards to employee policies and operating procedures, we maintain constant vigilance where your privacy is concerned.

Our firm always:

- Protects against reasonably anticipated threats or hazards to the security or integrity of client records and information
- Ensures that the investment advisor safeguards confidential client records and Information

and

- Protects any records and client information the release of which could result in harm of inconvenience to any client

Security of Client Assets
KGH, its Registered Representative, and its Investment Advisor Representative(s) DO NOT take, have, or maintain custody of any client assets.

Physical Security
At our office in Marion, VA, our physical security procedures are that visitors must always be escorted when on the premises and may not enter a office/room where the physical records, digital records, and/or the firm's computer equipment are located without the Investment Advisor Representative/Registered Representative/Chief Compliance Officer. Office/Storage Area/Room where client's physical records are stored, is and always must be locked behind a door of a structure's stationary wall; when not occupied by the firm's Investment Advisor Representative/Registered Representative/Chief Compliance Officer. Computer equipment used in the process of conducting business/records storage, for/as Kravitz Group Holdings, must have a lock screen with password activated (when not in use), anti-malware/spyware, firewall, and Anti-virus computer software/apps in use. Digital copies of all client records are stored on a cloud-based platform and on a physical computer protected with a password. Video surveillance and other electronic measures may be deployed throughout the office premises.

Cybersecurity & Technological Security Policies
Our technological systems are monitored for signs of tampering or unauthorized activity. We employ the use of encryption/virtual private networks/cloud-based platforms within and as our cybersecurity procedures. Kravitz Group Holdings, conducts penetration/vulnerability testing, and implements the latest firewall and antivirus technology. Email monitoring is also utilized for regulatory and compliance

purposes in order to protect our clients. We also maintain strict controls to limit and monitor employee access to our systems.

Our information technology professionals constantly research and develop enhancements to keep us at the vanguard of data security. We may deploy a team of independent auditors to review our technological systems.

Incident Response
Kravitz Group Holdings has procedures to prevent and detect intrusion, including an incident response plan. Our incident response plan is to ensure that appropriate technology and resources will be dedicated and utilized to the monitoring, prevention, and resolution of cyber security threats.

Technology Risk Management
Confidentiality, integrity, and availability of our systems and client data are of the upmost importance to Kravitz Group Holdings. To reduce the risk associated with threats and vulnerabilities, Kravitz Group Holdings employs procedures to protect our systems and data according to their sensitivity and criticality. IT risk assessments are continuously performed, and any outstanding remediation items are actively monitored.

Employee Training
Our employee policies emphasize the importance of preserving confidentiality. Newly hired associates will receive an employee handbook that provides comprehensive information about our privacy policies and procedures, together with security-awareness training. In addition, employees may attend training sessions on ethics and security. Our Registered Representative and/or regulatory compliance specialists will ensure that we meet federal requirements to preserve clients' privacy.

All financial advisors whom become affiliated with Kravitz Group Holdings will also receive training about our privacy policies and procedures.

Business Continuity
Our Registered Representative focuses on preparing for potential business disruptions due to unforeseen circumstances such as natural disasters. Their goal is to ensure that critical operations continue and data remains secure during emergencies. The Registered Representative/Chief Compliance Officer oversees management of our emergency functions such as data retention, backup procedures and off-site information storage. See the Disaster Recovery Plan for more information.

Industry-wide Coordination
Kravitz Group Holdings, coordinates with industrywide organizations and law enforcement agencies devoted to sharing information about physical and cybersecurity.