

## LEGAL NOTICES

### I. **GENERAL**

Welcome to the Code Advisors LLC (“CODE”) Internet Site (the “Site”). Please note the following disclosures and disclaimers.

CODE is registered as a broker-dealer with the Securities and Exchange Commission and is a member of the Financial Industry Regulatory Authority, as well as a member of the Securities Investor Protection Corporation. Please visit [www.finra.org](http://www.finra.org) and [www.sipc.org](http://www.sipc.org) for more information.

No portion of this Site is intended as an offer to sell or a solicitation of an offer to buy any securities. This Site is not intended for any use that would be contrary to law or regulation. If you have any questions about this Site, please contact CODE’s Legal and Compliance Department at 415.659.8088.

### II. **PRIVACY POLICY**

CODE is committed to safeguarding the confidential information of its clients. CODE holds all information provided to us by our clients and vendors in the strictest of confidence. CODE will only disclose information to non-affiliated third parties as permitted by law. CODE’s policy with respect to personal information about clients is as follows:

#### **The Information CODE Collects about Clients**

The non-public personal information that CODE collects about its clients comes primarily from its clients.

#### **How CODE Protects Personal Information**

CODE limits employee access to information only to those who need to know in order to provide service to clients, and only to nonaffiliated parties as permitted by law. CODE maintains physical, electronic, and procedural safeguards that are designed to comply with federal standards to guard client information.

#### **CODE’s Disclosure Policies**

CODE does not disclose client information to anyone, except as permitted by law. This may include sharing client information with non-affiliated companies that perform support services for client accounts.

#### **Opt-Out Policy**

Clients may opt out of the disclosure of non-public personal information to a non-affiliated third party by giving CODE notice in writing or email. CODE’s Chief Compliance Officer will maintain a list of individuals who have chosen to opt out. The list will contain the names of the individuals and the date that the opt-out notice was received.

If the CODE-client relationship ends, CODE will continue to treat the information as described in this Privacy Notice. CODE will dispose of all consumer report information via secure means, such as by shredding or by contracting with a third-party to dispose of the information in accordance with requirements.

Consumer report information means any record about an individual, whether in paper, electronic or other form, which is a consumer report or is derived from a consumer report. Consumer report information also means a compilation of such records.

#### **Safeguards**

CODE safeguards client information as follows:

#### **Desk Top and Lap Top Computers**

Computers are encrypted and require a password in order to access data. CDs, flash drives and other devices are generally stored in the locked offices of CODE.

#### **Removal of Client Information from Electronic Devices**

## **LEGAL NOTICES**

Client information will be removed from electronic devices including CD, flash drives, etc. prior to discarding the devices.

On an annual basis, CODE will retain an independent IT consultant to test the CODE computer systems. The test will detail the firewalls and systems that are in place to safeguard client information and prevent CODE systems from being accessed by unauthorized persons.

### **Storage of Physical Files**

CODE maintains storage facilities within its offices that are not accessible to the general public. Client files are maintained in filing cabinets in locked offices. Client information is accessed on a need to know basis by designated registered representatives and principals.

### **Incoming and Outgoing Mail**

All incoming and outgoing mail is processed through one location in the CODE office. Upon receipt, mail is immediately distributed to the appropriate principal for review and distribution. Outgoing mail is kept in an area that is not accessible to the general public.

### **New Technologies**

CODE's Financial and Operations Principal (the "FINOP") will be responsible for conducting due diligence on any new technologies utilized by CODE to ensure that implementation and utilization of the technology will safeguard client information.

The FINOP or his designated representative will be responsible for training its representatives and or employees on any such new technologies implemented by the Firm, including any related regulatory rules or regulations. Due diligence and training material will be maintained by the FINOP. If training is required, the FINOP will prepare written confirmation of the training date(s), attendees, and information that was presented by the FINOP or his designee.

## **III. BUSINESS CONTINUITY PLAN**

In the event of any disruption of our business, the safety and security of our employees and protection of customer information are our first and foremost concerns. Once safety and security have been addressed, we will ensure that business operations resume as quickly as possible by securing access to key documents, systems and data.

CODE's business continuity plan addresses several levels of potential business disruption, or "incidents". This summary contains information as to how the firm will resume business operations at each of the following levels of disruption:

Level 1 - loss of a mission critical system

Level 2 - facilities unavailable for one day or less (e.g., power outage)

Level 3 - facilities unavailable for greater than one day (e.g., fire)

Level 4 - regional impact event (e.g., earthquake)

Level 5 - incapacitation of firm's principals

### **Loss of a Mission Critical System or Data**

CODE has identified which systems and data are integral to daily operations and implemented a combination of back-up systems and secure off site data storage to assure that operations will continue without significant disruption.

### **Loss of Facilities**

CODE has made arrangements for both short term and longer term relocation of our employees and operations should our facilities become impaired. The combination of back-up systems and secure off site data storage will allow CODE employees to work from remote locations while the firm recovers critical documents either physically or electronically.

## **LEGAL NOTICES**

### **Regional Impact Event**

CODE's employees may be forced to relocate to other parts of the country should a large regional event occur. The firm maintains data in secure off-site locations outside of the Bay Area; the data is therefore likely to be available during such an event. Restoration of data should be complete within 24 to 48 hours.

### **Incapacitation of Firm's Principals**

CODE has arrangements in place to assure that, through a combination of in-house back-up and third party professionals, all of the firm's obligations to customers and regulators will continue to be met without interruption in the event of incapacitation of the firm's principals.

### **Testing and Updating of Plan**

CODE performs periodic testing of key elements of the business continuity plan. In the event of major changes in the firm's operations or principals, the plan will be updated as required.