## How Helm Investment Management Protects Your Confidential Information

Helm Investment Management, LLC ("Helm" or the "Firm") understands the importance of the trust that our clients place in us to maintain the confidentiality of their personal information. As noted in our Privacy Policy, we maintain physical, electronic and procedural safeguards to ensure that personal information is protected and not disclosed to any outside parties unless required by law. Furthermore, Helm's principals are CFA charterholders and are bound to adhere to the CFA Institute Code and Standands, which requires a preservation of confidentiality for clients, former clients, and prospective clients (Standard III(E)).

Physical safeguards include restricting access to our offices and computer servers, maintaining confidential client records in locked file cabinets or desk drawers, shredding sensitive documents prior to disposal, and, to the best of our ability, a limitation of unnecessary physical paperwork containing confidential information.

Regarding electronic, and electronically-stored information, Helm maintains a secure server and limits access to sensitive electronically-stored data only to personnel that have a business need to access that data. Our server is backed up on a daily basis to a cloud-based server which employs the highest security protocol. For the most sensitive data transmissions, we encourage clients to submit documentation via facsimile or secure e-mail. In the event that we need to use unencrypted e-mails, we truncate and/or redact account numbers and other sensitive information before transmission.

In addition to our on-site policies for the protection of sensitive electronic information, we also have policies in place to ensure that any offsite access to confidential client information is protected. With the assistance of our third-party information technology consultant, we have set up secure remote-access ("VPN") for the Firm's principals. VPN connections are accessed through a secure portal and only allowed to be initiated via a secured internet connection. The Firm's principals also maintain cellular phone devices for business use. Helm requires that these devices are password-protected. At no time is sensitive client information allowed to be stored on personally-owned computing or mobile devices.

Procedural safeguards of client information relate primarily to the manner in which Helm principals, employees and contractors utilize confidential client information. At a minimum, Helm principals, employees and contractors at all times adhere to the Firm's code of conduct, as well as the physical and electronic safeguards noted in the paragraphs above. Additional procedures apply to trading, the handling of physical cash, checks and securities, and the transfer of funds and securities to internal and external accounts.

Trading authorization is only granted to Helm principals and all trades are entered into a "trade blotter" and reconciled upon final trade settlement. Any trading errors are immediately to be brought to the attention of the Firm's chief compliance officer and corrected as soon as practicable with no adverse outcome for the client.

Any client checks or securities delivered in physical form to the Helm office are to be immediately transferred to the custodian for that client's account(s). All checks are to be made out to the custodian and not to Helm. Helm employees are instructed to never accept cash.

Any checks or physical securities that cannot be delivered to the custodian on the same business day will be stored in the firm safe and deposited the following business day.

The vast majority of the transfer of funds and securities is conducted electronically through the secure websites of the client's preferred custodian. It is Helm's strong preference for clients to set up direct links to their banking accounts through their preferred custodian. In the rare instance where the client does not have a direct link to an outside account, and no other option will suffice aside from a wire transfer, the following rules apply. First, the wire may only be initiated by a principal of the Firm. Second, the principal initiating the wire must speak with the client, in person or via the telephone. During that conversation, the Helm principal must verify the client's identity, either visually in person, or on the telephone by initiating an outbound call to the phone number of record in Helm's files. During that phone call, the Firm principal must verify that he or she is speaking with the client that has requested the wire transfer. In both in-person and telephone conversations regarding wire transfers, the Helm principal must confirm the wire amount, account to be debited and account to be credited.