GUIDING PRINCIPLES

Geneva Capital Management ("Geneva", "Company" or "Firm") is committed to protecting the confidentiality and security of the personal information we collect about clients. The purpose of this policy is to outline the practices developed by Geneva to safeguard client non-public personal information and to protect against fraud, unauthorized transactions, claims or other liability. This policy applies to current and former clients.

STATEMENT OF POLICY

Privacy rules adopted under the Gramm-Leach-Bliley Act, Regulation S-P[1], require that Geneva take the following actions:

1) Establish appropriate standards to protect customer information;
2) Restrict disclosure of non-public personal information about customers; and
3) Provide customers with a notice of its privacy policies and practices.

Personal information is defined as non-public, personally identifiable financial information or any list, description or other grouping of customers that is derived using any personally identifiable financial information ("Confidential Information") including, but not limited to, the following:

- Client identity including name, address and age;
- Social Security Number;
- Financial account information including account numbers, account titles, PIN numbers, etc., the improper disclosure of which could facilitate unauthorized access to client accounts, identity theft or fraud; and
- Client financial information such as assets, income, net-worth, account balance(s), bank account information, beneficiary information, investment activity and other investments.

Geneva employs physical, electronic, technological, and other safeguards designed to keep Confidential Information safe while in our possession and upon destruction.

Physical and Other Safeguards

- Employees are issued building/suite key access/proxy tokens with the appropriate access level initially upon employment.
- All doors that provide entry to Geneva's office are access-controlled – they require a secure access token to gain entry and automatically close and lock after each opening.

[1] Because Geneva only collects person information of the types covered by the Gramm-Leach-Bliley Act ("GLBA"), it is exempt from the application of the California Consumer Privacy Act ("CCPA") to such personal information. See CCPA §1798.145(e). GLBA entities remain subject to the CCPA if they engage in activities falling outside of the GLBA. Examples include using targeted online advertising, tracking web page visitors and/or collecting geolocation data – none of which occur at Geneva. Furthermore, GLBA-regulated entities remain subject to potential damages under the CCPA §1978.150 if they experience a data breach.

- Each Employee is responsible for locking file cabinets that contain Confidential Information. Geneva has designated a specific employee who is responsible for locking common area file cabinets and securely storing file cabinet keys at the close of business each day. Most Confidential Information is now saved into secure electronic files, so access to file cabinets containing paper Confidential Information is infrequent.
- Employees are prohibited from leaving documents containing Confidential Information unattended at the front desk or in other common work areas.
- Employees are prohibited from discussing Confidential Information about clients or client accounts in public areas. Discussions among employees must take place in private, confidential locations within the office and building.

Technology and Electronic Safeguards

- Geneva's IT manager (Halcyon Financial Technology, L.P.) is responsible for establishing and maintaining system passwords and other security settings and access controls on Company issued computers, system drives, mobile devices, network, cloud and internet-based applications and other devices.
- Employees are prohibited from changing the security settings assigned by the IT manager.
- Employees are required to keep password information strictly confidential and prohibited from openly displaying or sharing password information with co-workers.
- Geneva's IT manager is responsible for all aspects of Geneva's cybersecurity controls, including establishing and monitoring network firewall protection, system security to reasonably prevent infiltration by unauthorized outside parties, assessing system vulnerabilities, and recommending and implementing security patches and upgrades.
- Geneva's IT manager and Geneva have implemented policies relating to remote access and the use of mobile and personal devices by employees.
- Geneva's CCO is responsible for establishing procedures to prevent unauthorized access to Geneva's physical records and Geneva's IT manager, upon receiving notification of a departure, is responsible for preventing unauthorized access to electronic records upon termination of an employee.

Information Handling and Destruction

- Geneva requires the use of a professional service to destroy all paper documents or forms that contain Confidential Information that are no longer useful; the Firm maintains evidence of destruction.
- Employees are required to dispose of all paper documents containing Confidential Information in a secure receptacle provided by the document destruction service; Employees are prohibited from disposing of documents or forms that contain Confidential Information in regular trash receptacles.
- Geneva's IT supervisor is responsible for disposing of retired computers, hard drives, and other Company equipment that are no longer used.
- Employees are prohibited from removing Confidential Information from office premises except in connection with documents used for client meeting purposes or as otherwise described herein. No other Confidential Information may be removed from office premises

without prior approval by the Compliance Department. Aged and closed files containing Confidential Information may be stored at a secure off-site storage facility and destroyed by the facility in accordance with Geneva's document retention and destruction policies.

Remote Access Safeguards – Mobil Devices

Geneva's IT manager is responsible for providing employees with access to remote connectivity on mobile devices. Geneva's Information Technology Security Policy provides that only mobile devices (company owned, personal or third party) that adhere to Geneva's security standards will be granted access. Processes are in place for requesting authorization and the prompt removal of mobile device access once the access is no longer authorized or required.

Remote Access Safeguards – Work-from-Home

- Systems Access. Geneva's IT manager is responsible for providing and monitoring employees' remote access of company applications and data on both Company and personal computers. All remote access will be provided through Citrix, Microsoft Remote Desktop or a similarly secure application and connect to the Company through the Internet using a VPN or similarly secure connection.

- Company Data on Work Computers. Employees may only save Company data onto their Geneva network drives and Company computers. Employees working remotely are blocked from directly saving any Company data locally onto any non-Geneva computers or other devices. Geneva and the IT manager will continue to maintain all the access controls described in this policy and Geneva's Information Technology Security Policy.

- Minimize Printing Confidential Information. Printing of documents containing Confidential Information should only occur to the extent necessary to complete assigned tasks and responsibilities. Any printed documents containing Confidential Information must be disposed of as described herein – either at Geneva's office through in a secure receptacle provided by a document destruction service or through a document shredder. Employees are prohibited from disposing of documents that contain Confidential Information in regular trash receptacles.

- Access Control. Employees working from home will maintain the same safe conditions, security and safety habits at their home office as are established for Geneva's office.

Outside Vendors

Outside vendors are used by Geneva to assist in the performance of a variety of critical activities and maintain corresponding records – including client accounting, trading, billing, and performance measurement. All material vendor contracts are reviewed by Geneva's CCO and vendors that provide computer-based products are reviewed by Geneva's IT manager for adherence to Geneva security and confidentiality requirements. Geneva maintains an inventory of vendors who hold Confidential Information.

Training

Geneva requires employees to complete annual training that includes privacy-related topics. Geneva includes information concerning its Privacy and Confidential Information Policy in ongoing employee training activities.

Information Technology Policies

Geneva has worked without its IT manager to develop processes, systems and controls designed to protect computer systems and data privacy. The following policies and procedures apply to Geneva and its electronic information:

- Information Technology Security Policy. This policy document has been prepared to ensure the adequate protection of business data and business information systems throughout Geneva. It is also intended to underscore Geneva's commitment to integrity and high-quality business relationships with its clients, employees, vendors and other business partners.

- Information Technology Incident Response Process. This document is designed to provide the guidelines and processes to follow in the event of a security incident and/or security breach.

- Computer Information and Systems Usage Policy. This policy describes in greater detail permissible and impermissible uses of Company systems and includes provisions designed to protect system security and confidential information.

Incident Response

Geneva employees are required to report any observed or suspected security weaknesses, or threats to, information systems to their managers and/or to Geneva's IT manager as soon as possible. Additional guidance is found in the Security Incident Response Process.

In the event of an incident involving a potential unauthorized release of Confidential Information, Geneva's CCO and Head of Operations will be promptly notified. The CCO or Head of Operations will contact the IT manager and, if the breach involves any computer systems, activate its Information Technology Incident Response Process. Geneva will work with the IT manager to determine the appropriate steps to analyze, contain, and mitigate the incident. Depending on the circumstances, Geneva may be required to notify regulators within any required time frames and, depending on the severity of the breach, notify clients.

DISCLOSURE OF NON-PUBLIC PERSONAL INFORMATION

In order for Geneva to provide investment management services to clients, disclosure of Confidential Information is required in very limited circumstances. Employees may share client Confidential Information in the following ways:

- Disclosures to companies that require access to client personal information to perform services on our behalf (such as the provider of Geneva's client accounting, billing and trading systems and other similar authorized vendors, and auditors who verify our performance calculations). Geneva, through its vendor contract review process, is responsible for obtaining confidentiality agreements from vendors who use or obtain access to Confidential Information in the performance of services to Geneva;

- Disclosures to companies that help us process or service client transactions or account(s) (such as providing account information to brokers and custodians);
- Disclosures at client request to attorneys, accountants, and other client representatives;
- As permitted or required by law;
- As requested by a client; and
- Disclosures of client names on lists of representative clients if such clients grant written consent to such disclosure.

ELECTRONIC COMMUNICATIONS WITH CLIENTS

Client statements and other confidential information, along with meeting materials, are typically sent to clients and their representatives by regular or express mail. However, some clients and representatives may request that their materials be sent via email. In such cases, Geneva will send the materials in an encrypted document, typically a password protected PDF file, and the password will be sent to the client in a separate email. Other methods of information encryption may be also used as technology evolves and becomes widely available.

Except when sending materials to clients in the manner described above, employees are prohibited from sending Confidential Information to unsecure locations outside Geneva's computer network. An example of prohibited activities includes sending Confidential Information to an employee's personal email account or to unauthorized data storage or file sharing servers.

No client mobile phone information will be shared with any third parties or affiliates for marketing or promotional purposes. Certain clients, consultants and prospects may choose to text Geneva via Geneva's Zoom text account. All such texts will constitute consent to receiving text messages from Geneva and will be retained in accordance with Geneva's recordkeeping policies and procedures. Geneva does not initiate marketing or promotional text messages to clients or others. Geneva does not do A2P (application-to-person) messaging – aka SMS business. Should Geneva choose to engage in SMS marketing with clients or prospects, it will first obtain their written consent to receive such text messages.

NOTICE OF PRIVACY POLICIES AND PRACTICES

Regulation S-P, among other things, requires Geneva to: (1) provide a clear and conspicuous notice to its customers that accurately reflects its privacy policies and practices generally no later than when it establishes a customer relationship ("Initial Privacy Notice"), (2) provide a clear and conspicuous notice to its customers that accurately reflects its privacy policies and practices not less than annually during the continuation of the customer relationship ("Annual Privacy Notice," and together with the Initial Privacy Notice, "Privacy Notices"), and (3) deliver a clear and conspicuous notice to its customers that accurately explains the right to opt out of some disclosures of non-public personal information about the customer to nonaffiliated third parties ("Opt-Out Notice"). Regulation S-P describes the information that must be included in Privacy Notices, including the categories of nonpublic personal information that Geneva collects and discloses, and in Opt-Out Notices, if applicable.

- Geneva's Operations Department is responsible for providing all current clients with a copy of Geneva's Initial Privacy Notice, Annual Privacy Notice, any required updates following a material revision of the policy.

- Geneva's Operations Staff must provide Geneva's Privacy Notice to all new and prospective clients at initial meetings or along with account opening paperwork.

Geneva's Privacy Notice is considered a part of this policy. The Compliance Department is responsible for overseeing Geneva's privacy practices. Employees aware of any potential breaches of this policy should inform Compliance immediately. Questions concerning confidentiality issues should be directed to the CCO.

Policy Date: 2004-10-05
Revised: 2005-03-02
2008-06-24
2009-04-23
2010-10-15
2013-11-12
2015-10-30
2016-10-01
2017-08-01
2019-05-28
2020-03-18
2020-09-04
2024-07-30