TIMONIER

The confidence and trust of our clients is our most important asset and we are committed to safeguarding your privacy and the confidentiality of your personal information. Below are the details of our privacy policies which explain the collection, use and retention of your confidential data.

I. All information collected regarding any client and recorded on any firm document, correspondence, electronic medium or other way, including hand written notes, shall be protected and not made available to any non-employee of the firm without permission of the client.

II. All documents, correspondence and other materials containing client personal information must be kept in files, and those files must be securely retained. Personal information will not be left on desks or in places available for third parties to view.

III. All computers may be accessed only by employees for business purposes.

IV. No information relating to a client's business may be transferred to a non-office computer.

V. All company owned work machines will require a cyber security applet, Advisor Armor.

VI. All company owned work machines are required to have the latest version of commercial antivirus and malware prevention software, Sentinel One.

VII. All company owned work machines are required to have enabled Firewall, screen lock for idle systems, BitLocker Drive Encryption, and disabled remote login.

VIII. All company owned work machines are required to update their operating systems and software up to date and to include the latest fixes and preventative measures.

IX. All employees are forbidden from selling or distributing any client information.

X. Any firm records held beyond legally required retention periods under federal and state law must be destroyed by shredding or some other means which destroys the file, document or other item completely. No record may be destroyed without the advance consent of the Chief Compliance Officer.

XI. Generally, all records should be retained and used at the firm's offices and not taken from the office except during meetings with clients when document reviews are necessary. When removed from the office, client personal information should be transported in a way that does not allow any information to be viewed by third parties.

XII. The office must be locked at all times when employees are not present.

XIII. No employee may discuss the business or background information of any client with a third party, even casually, unless the discussion occurs for business purposes and with the prior permission of the client.

XIV. All software programs containing client personal information are password protected and passwords are revised and updated on a regular basis. Any outbound email correspondence that contains personal information shall be encrypted via Erado/2ix.

XV. Any departing employee may not take confidential information in any format.

We consider privacy, security and service to be an integral part of our business. As always, we welcome your questions and feedback.

Best Regards,

Nicholas C. Baker

Nicholas C. Baker, AAMS®