EQIS REINVENTING WEALTH MANAGEMENT

1000 4th St., Suite 650
San Rafael, CA 94901
Phone: 800.949.9936
Fax: 630.206.0757
www.eqis.com

COMPREHENSIVE WRITTEN INFORMATION SECURITY PROGRAM - (WISP)

WISP

I. OBJECTIVE:

Eqis Capital Management, Inc.'s objective, in the development and implementation of this comprehensive written information security program ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personal information. The WISP sets forth our procedures for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information. "Personal information" in this context is defined to include the first name and last name or first initial and last name in combination with any one or more of the following related elements : (a) Social Security number; (b) driver's license number or state-issued identification card number; (c) financial account number, or credit or debit card number, with or without the required security code, access code, personal identification number or password, that would permit access to a resident's financial account (provided, however, that "personal information" shall not include information that is publicly available from federal, state or local government records lawfully made available to the general public). This WISP is designed to protect against the unauthorized disclosure of personal information of our clients and employees that is in our possession.

II. PURPOSE:

The purpose of this WISP is to: (a) Ensure the security and confidentiality of personal information (b) Protect against any anticipated threats or hazards to the security or integrity of such information and; (c) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE:

The WISP should:

1. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information.

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information.

3. Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.

4. Design and implement a WISP that puts safeguards in place to minimize those risks, consistent with the industry standards.

5. Regularly monitor the effectiveness of the safeguards.

IV. DATA SECURITY COORDINATOR:

We have designated Jennifer Winters, to implement, supervise and maintain the WISP. That designated employee (the "Data Information Security Manager ("DISM") will be responsible for: (a) Initial implementation of the WISP; (b) Training employees; (c) Regular testing of the WISP safeguards; (d) Evaluating the ability of each of our third party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them to have access, and requiring such third party service providers by contract to implement and maintain appropriate security measures; (e) Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information; and (f) Conducting an annual training session for all owners, managers, employees and independent contractors, including temporary and contract employees who have access to personal information on the elements of the WISP. All attendees at such training sessions are required to certify their attendance as well as their familiarity with the firm's requirements for ensuring the protection of personal information.

V. INTERNAL RISKS:

In order to combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and for purposes of evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately.

Internal Threats

A copy of the WISP must be distributed to each employee who shall, upon receipt, acknowledge in writing that he/she has received a copy.

There must be immediate retraining of employees on the detailed provisions of the WISP.

Employment contracts must be amended immediately to require that all employees comply with the provisions of the WISP, and prohibit any nonconforming use of personal information during or after employment. The WISP must provide for mandatory disciplinary action to be taken for violation of security provisions of the WISP. (*The nature of the disciplinary measures may depend on a number of factors including the nature of the violation and the nature of the personal information effected by the violation)*.

The amount of personal information collected should be limited to that amount reasonably necessary to accomplish our legitimate business purposes, or that is necessary for us to comply with other state or federal regulations.

Access to records containing personal information shall be limited to those persons who are reasonably required to know such information in order to accomplish legitimate business activities or to enable us to comply with other state or federal regulations.

Electronic access to user identification after multiple unsuccessful attempts to gain access must be blocked.

All security measures shall be reviewed at least annually, or whenever there is a material change in our business practices that may reasonably implicate the security or integrity of records containing personal information. The Data Security Coordinator shall be responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.

Terminated employees must return all records containing personal information, in any form, that may at the time of such termination be in the former employee's possession (including information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)

A terminated employee's physical and electronic access to personal information must be immediately blocked. Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the firm's premises or information.

Such terminated employee's remote electronic access to personal information must be disabled including his/her voicemail access, e-mail access, internet access, and passwords must be invalidated, and surrender of all keys, IDs or access codes or badges that permit access to the firm's premises or information; and the return of all records containing PI whenever an employee leaves the firm. The Data Security Coordinator shall maintain a highly secured master list of all lock combinations, passwords and keys.

Current employees' user IDs and passwords must be changed at least once a year.

Access to personal information shall be restricted to active users and active user accounts only.

Employees are encouraged to report any suspicious or unauthorized use of customer information.

Whenever there is an incident that requires notification, there shall be an immediate mandatory post-incident review of events and actions taken, (if any), with a view to determining whether any changes in our security practices are required.

Employees are prohibited from keeping open files containing personal information on their desks whenever they are absent from their desks for nominal periods of time to be defined as 15 minutes.

Employees are prohibited from using their personal, non Eqis issued electronic devices including cell phones at their desk. All personal phone calls taken on such devices shall be taken outside the office so as not to disrupt the working environment. Use of personal electronics for browsing, texting, checking email, etc may not be done at your desk. Use of such devices, with the exception of phone calls, is allowed in the break room. This policy is in place for the protection of Eqis and our clients.

At the end of the work day, all files and other records containing personal information must be secured in a manner that is consistent with the WISP's rules for protecting the security of personal information.

Each department shall develop rules (bearing in mind the business needs of that department) that ensure that reasonable restrictions upon physical access to records containing personal information are in place, including a written procedure that sets forth the manner in which physical access to such records is to be restricted; and each department must store such records and data in locked facilities, secure storage areas or locked containers.

Access to electronically stored personal information shall be electronically limited to those employees having a unique log-in ID and re-log-in shall be required when all computers have been inactive for more than a few minutes. Computer users must set their computers so that they require the use of a password to use them whenever they are not in use for 15 minutes.

Visitors' access must be restricted to one entry point for each building in which personal information is stored. Visitors shall not be permitted to visit unescorted any area within our premises that contains personal information.

Paper or electronic records (including records stored on hard drives or other electronic media) containing personal information shall be disposed of only in a manner that is consistent with industry standards.

VI. EXTERNAL RISKS

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures must be followed by Eqis Capital Management, Inc.

Limiting Access to Records Containing PI:

All paper documents containing PI must be secured in a locked cabinet and/or office when not in use. Keys should be distributed only to those individuals authorized to have access to such records.

Safeguard firm's computer systems with "up-to-date" firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, installed on all systems processing personal information.

Practice the use of reasonably up-to-date versions of system security agent software which includes malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing personal information.

To the extent technically feasible, all personal information stored on laptops or other portable devices must be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible. Encryption as defined in this document means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

All computer systems must be monitored for unauthorized use of or access to PI.

There must be secure user authentication protocols in place, including:

1. Protocols for control of user IDs and other identifiers.

2. A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies (such as biometrics or token devices). Eqis maintains the use of strong passwords (standards include a minimum of 8 characters, including at least one non-letter character and at least one change of case) that are periodically changed, at least once a year and whenever an employee leaves.

3. Control of data security passwords to ensure that such passwords are kept in a secure location.

Restrict access to PI to active users and active user accounts.

Eqis has established policies and procedures addressing when and how records containing PI may be transported off the firm's business premises, as well as requirements for securing such records during that time and ensuring the records are fully and safely returned to the business. If employees travel with records containing PI, establish well-defined procedures regarding the use of laptops, portable storage devices, and hard copy records to safeguard those records against theft and loss. Eqis maintains user ID and password protection of such devices.

Eqis restrict visitors' access to the firm and particularly to areas of the firm where PI is stored. Visitors may not visit any area containing such information unescorted.

Monitoring & Periodic Testing

Eqis maintains practices that attempt to monitor and test the firm's procedures.

Eqis will regularly monitor, test and review system logs, virus scanners and intrusion-detection systems.

Eqis will randomly review employees' offices/work areas to ensure that no records containing PI are left unattended during office hours, or are not secured at the end of the business day.

Eqis will conduct an inventory of software and security systems installed on company issued and/or employees' personal laptops (if used for business purposes) on at least an annual basis.

Eqis will conduct a review of firm's security measures at least annually, or whenever there is a material change in the firm's business practices that may affect the security or integrity of PI records.

Eqis will require departments to conduct periodic reviews of records containing PI to identify records that can be destroyed consistent with firm policies and in compliance with state or federal regulations.

Analysis of Third Party Service Providers

Eqis will attempt to ensure that all third party service providers are maintaining appropriate security measures consistent with 201 CMR 17.00 and applicable state or federal regulations. Effective March 1, 2010, third party service providers are required to provide such confirmation contractually.

Eqis will review and revise (if necessary) firm's contracts with such vendors to include provisions allowing for on-site visits or other forms of monitoring as appropriate (i.e., due diligence reviews).

Eqis will obtain copies of vendors' SAS 70 reports, annual compliance reviews, and require immediate reporting of any security breaches or regulatory violations.

Security Breach Response Procedures

Eqis will establish a data security breach team, which should include senior management and staff from the firm's compliance, legal, IT and human resources departments, at a minimum. Breaches will be dealt with individually and appropriately.

Eqis has created draft notices and notification protocols, including business partners and regulators, where necessary. Due to the potential risks to the Eqis' reputation as well as any financial consequences resulting from a security breach, Eqis will work closely with our legal counsel from the outset to ensure that such matters are handled appropriately.

Eqis may implement possible ways to notify and answer questions via a toll-free call-in number and/or a website FAQ (frequently asked questions) page that can be quickly implemented in the event of a breach.

Eqis will promptly conduct a mandatory post-incident review of the event and actions taken, if any, to determine whether any changes are warranted to the firm's security practices.