Cyber Security & Information Security Policy

Inventory of Technology Infrastructure

On an annual basis, the CCO of EWP will make an inventory of the following:

- Physical devices and systems (computers, servers, etc.);
- Software platforms and applications (email applications, file management, etc.);
- Systems that house client data; and
- Third-party contractors that have access to systems, platforms, etc.

EWP's primary software platforms that may contain client data are summarized below.

Type of System	Name of System
Customer Relationship Management (CRM)	SalesForce
Email Provider / Hosting	Appriver
Email / Social Media Archiving	Smarsh
Document Management / Storage	Egnyte

EWP utilizes cloud-based technology systems, which it believes provide increased information security capabilities including:

- Ability to leverage the established infrastructure of trusted technology industry leaders; and
- Improved system alert capabilities including better user activity logging and alerts related to unusual user activity.

EWP also recognizes that cloud-based technology systems create a greater reliance on passwords and user login security. As such, EWP has designed and will continue to further develop information security policies with this increased risk as a focus.

Detection of Unauthorized Activity

The CCO is responsible for monitoring on-site and cloud-based systems for suspicious activity. Such activity may include:

- Logins to company systems after traditional business hours for the local region;
- Logins to company systems from non-local regions; and/or
- Large transfers of files or data.

When suspicious activity is discovered, the CCO will restrict access to the systems and begin to assess what information may have been accessed and what actions need to be taken to remediate the event.

If the unauthorized activity is deemed by the CCO to have led to unauthorized release or use of sensitive client information, the CCO will contact the proper law enforcement and/or regulatory agencies as required by state and federal law.

Regardless of the severity, the CCO will keep a log of suspected unauthorized activity and note the action taken. This log will include the following information about each incident:

- Date and time of the incident;
- How the incident was detected;
- The nature and severity of the incident;
- The response taken to address the incident; and
- Any changes made to the Information Security Policy as a result of the incident.

In addition, all staff should immediately alert the CCO of any suspicious behavior or concern.

Prevention of Unauthorized Funds Transfers

EWP has implemented the following firm-wide information security polices to help prevent unauthorized funds transfers:

- Clients must confirm wire requests verbally. Wire requests may not be authorized solely via email; and
- Wire requests should be reviewed for suspicious behavior (e.g. time of request, atypical amount of request, etc.).

EWP is particularly aware of the risk caused by fraudulent emails, purportedly from clients, seeking to direct transfers of customer funds or securities and will train staff members to properly identify such fraudulent emails.

User Login Security

EWP has implemented the following firm-wide user login security polices to help prevent unauthorized access to sensitive client data:

- Computers used to access client data will have antivirus software installed. In addition, the antivirus software must have an active subscription and updates must be scheduled to automatically install;
- Staff will utilize devices with up to date operating system software with all security patch and other software updates set to automatically install;
- Staff members are prohibited from accessing EWP systems from unsecured internet connections;
- All staff passwords are required to meet or exceed the following guidelines:
  - Contain both upper and lower case letters;
  - Contain at least one number;
  - Contain at least one special character;

    - Be at least 10 characters in length;
    - May not contain words that can be found in a dictionary; and
    - May not contain personal information such as pet names, birthdates, or phone numbers.
- All staff are required to have unique passwords to access each technology system (e.g. desktop computer, CRM system, etc.);
- All staff are required to update passwords on a quarterly basis;
- No passwords are allowed to be stored in writing on paper or on any system;
- Staff members should not use the "remember password" feature of any application;
- Staff members should never share passwords with any other staff member or 3rd party; and

When available, staff is required to utilize two-factor authentication.

User Access Privileges

EWP has implemented the following firm-wide user access privilege polices to help prevent unauthorized access to sensitive client data:

- All new staff members login credentials will be created by the CCO;
- Staff members will only have access to systems deemed necessary by the CCO;
- Staff members, besides the CCO or other designated personnel, will not have access to administrative privileges on systems unless deemed necessary by the CCO; and
- Upon a staff member's departure or termination, the CCO will immediately remove the former staff member's access to all firm systems.

Staff members may request additional access to systems by contacting the CCO.

Email Use Security and Guidelines

EWP has implemented the following firm-wide email use security polices and guidelines to help prevent unauthorized access to sensitive client data:

- All staff should only provide sensitive information electronically to clients via a secure email or client portal;
- All staff should never open or download any email attachments from unknown senders;
- All staff should never open or download any email attachments from known senders that look suspicious or out of the ordinary;
- All staff should never directly click on or open any links sent in emails; and
- All staff should be acutely aware of any attempted "phishing" emails seeking to obtain the staff member's user login credentials. Some warning signs to look for include:
    - Bad spelling or poor grammar in the email subject or body text;
    - An unfamiliar company or website that the staff member is not familiar with; and
    - A suspicious sender email domain.

When a staff member receives a suspicious email, the CCO should be immediately alerted. The CCO will then determine next steps and communicate to other staff members if deemed appropriate.

3rd Party Vendor Security and Diligence

EWP has implemented the following firm-wide 3rd party vendor security and diligence polices and guidelines to help prevent unauthorized access to sensitive client data:

- All 3rd party vendors that have physical access to the office and/or the firm's systems are required to enter into a non-disclosure agreement (NDA) in order to protect sensitive client information before establishing a business relationship; and
- Proper due diligence will be performed on all relevant technology vendors prior to establishing a business relationship and then again on at least an annual basis and will include:
    - Review of the firm's information security policies;
    - Review of the firm's disaster recovery policies; and
    - Review of the firm's general capabilities to ensure it meets EWP's needs.

All of this information will be stored and maintained in EWP's vendor diligence file.

Significant Technology System Disruption Plan

In the event of a significant business disruption that results in a significant interruption in access to the firm's technology systems, EWP will implement its business continuity plan as detailed in this policies and procedures manual.

Testing

On an annual basis, EWP will test its current information security policy and capabilities. The test conducted by the CCO will include the following activities:

- Attempt to access a random sample of firm devices to ensure that proper passwords are in place to prevent access;
- Attempt to access users' accounts with the proper password to ensure that two-factor authentication prevents system access;
- Attempt to restore a sample of files and records from the systems listed above to ensure that the restoration process is sufficient and properly configured; and
- Make a physical inspection of the office to ensure that all workstations have the proper security measures.

The results from the annual test will be documented and utilized as an opportunity to update the Information Security Policy.

Privacy Policy

The privacy policy statement is given to clients at the initial signing of the client contract and mailed or emailed with client consent once annually, if the policy is updated. The CCO will document the date the privacy policy was delivered to each client for each year if an annual delivery is required. EWP collects non-public personal information about clients from the following sources:

- Information it receives from them on applications or other forms;
- Information about their transactions with EWP or others; and
- Information it receives from a consumer reporting agency.

Below are the reasons for which EWP may share a client's personal information.

- For everyday business purposes – such as to process client transactions, maintain client account(s), respond to court orders and legal investigations, or report to credit bureaus;
- For marketing by EWP – to offer EWP's products and services to clients;
- For joint marketing with other financial companies;
- For affiliates' everyday business purposes – information about client transactions and experience; or
- For non-affiliates to market to clients (only where allowed).

If a client decides to close his or her account(s) or becomes an inactive customer, EWP will adhere to the privacy policies and practices as described in this Policies and Procedures manual, as updated.

EWP restricts access to clients' personal and account information to those employees who need to know that information to provide products or services to its clients. EWP maintains physical, electronic, and procedural safeguards to guard clients' non-public personal information.

The names of EWP's current and former access persons can be found in Exhibit 2.

In addition to EWP's listed access persons, any IT persons or other technical consultants employed at the firm may also have access to non-public client information at any time. An on-site or off-site server that stores client information, third-party software that generates statements or performance reports, or third-party client portals designed to store client files all hold the potential for a breach of non-public client information.

To mitigate a possible breach of the private information, EWP uses encryption software on all computers and carefully evaluates any third-party providers, employees, and consultants with regard to their security protocols, privacy policies, and/or security and privacy training.

The system is tested and monitored at least daily.

The test conducted by the CCO will include the following activities:

- Attempt to access a random sample of firm devices to ensure that proper passwords are in place to prevent access;
- Attempt to access users' accounts with the proper password to ensure that two-factor authentication prevents system access; and
- Attempt to restore a sample of files and records to ensure that the restoration process is sufficient and properly configured.

The results from the annual test will be documented and utilized as an opportunity to update the Information Security Policy.

Staff Training

On an annual basis, EWP will conduct a firm-wide training session to ensure that staff members are properly trained and equipped to implement the above policies. New staff members will receive training, led by the CCO, within 1 month of their initial hire date.

EWP uses various methods to store and archive client files and other information. Third party services or contractors used have been made aware of the importance EWP places on both firm and client information security. In addition to electronic and personnel measures EWP has implemented reasonable physical security measures at its home office location.

EWP will retain records for at least 5 years after the year in which the record was produced, or as otherwise required by law. With respect to disposal of non-public personal information, EWP will take reasonable measures to protect against unauthorized access to or use of such information in connection with its disposal.