Plan Confidence Corp Cyber Security Policy
March 2022

Safeguarding of Client Records and Information

- Prohibit an employee from providing client information over the telephone or in response to an e-mail message unless the employee has identified the other person as the client, a fiduciary representative of the client, an authorized agent of the client.
- All employees are required to utilize the predetermined secure and encrypted document service when handling sensitive client documents whether by uploading or downloading these documents.
- Maintain appropriate security measures for the computer and information systems.
  - System level and user level passwords must be strong - a password that is designed in a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to figure out.
    - Must be at least 7 characters, contain a mix of alpha and numeric, with at least one digit and should be more complex than a single word.
  - All computers must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes. Screens must be locked or logged off when the device is unattended.
  - Personal devices (e.g. smartphones, tablet, or laptops) used to access the network remotely must require a password to access. It is recommended but not required that this device has a firewall and antivirus software installed.
  - Dispose of client information stored in electronic or paper form in such a manner (e.g., through the use of a shredder) to reasonably ensure such information is protected from unauthorized access.
  - Where applicable, visitors and third-party service providers with access to sensitive client information will be supervised by at least one employee of PLAN CONFIDENCE.

Information Security Policy

Password Protection

It is of utmost importance that passwords remain protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different firm systems.
- Do not use the same password for systems inside and outside of work.

Third Party Vendors

Documentation

The following documents will be obtained, if available, in order for the firm to conduct a due diligence review and risk assessment of those vendors deemed mission critical.

- Contractual agreements or agreed upon terms of service.
- Privacy Policy

Review of documentation will be documents on PLAN CONFIDENCE’s Vendor Due Diligence/Risk Assessment Form.

Process

Vendor Due Diligence/Risk Assessment Forms will be initially compiled by Mark Reddick or Kevin Clark who will present the summaries to Kevin Clark, CEO & CCO for approval.

Vendor Access (Physically / Remotely)

Where applicable, visitors and third-party service providers with access to sensitive client information will be supervised by at least one employee of PLAN CONFIDENCE.

Remote access to PLAN CONFIDENCE’s system must only be granted to those vendors we are currently contracted with and who have addressed privacy and confidentiality within their vendor documents and/or have been approved by the Board.

Environment

Amazon Web Services (AWS), a comprehensive web services provider, is utilized by PLAN CONFIDENCE. AWS centralizes security to protect sensitive data and prevent data loss by hosting data in a cloud environment, not on individual devices, which reduces the risk of intrusion through insecure devices or network connections. The environment provided by AWS includes web servers, encrypted databases, secure document storage and daily database backups. Access to the PLAN CONFIDENCE AWS account is secured by limited functionality AWS accounts with strong passwords and multi-factor authentication as provided by AWS.

Stripe Payments (Stripe), an online credit card payment processing service provider, is utilized by PLAN CONFIDENCE. The PLAN CONFIDENCE implementation of the Stripe service has the client’s credit card information never touch the PLAN CONFIDENCE servers. When the PLAN CONFIDENCE payment web page is displayed in the client’s browser, the client enters their payment data into the web form on the web page. The credit card data (card number, expiration date and CVV security code) is then gathered by JavaScript that runs in the client’s browser directly (not on the PLAN CONFIDENCE servers) and that JavaScript then sends the credit card data to the Stripe servers over a secure and encrypted HTTPS connection. The Stripe servers process the credit card data and send back a token (code of random letters and numbers). This token represents that particular transaction on Stripe. JavaScript in the client’s browser then sends just that token to the PLAN CONFIDENCE servers which is stored in the secure and encrypted PLAN CONFIDENCE database alongside the rest of the client’s information that we store. The client’s credit card data never touches the PLAN CONFIDENCE servers. The client’s credit card data only ever resides in the client’s browser and sent encrypted from there to the Stripe servers.

Data Backups

Amazon AWS automatically creates secure backup copies of the PLAN CONFIDENCE database on a daily basis and retains 7 days of backups.

Client Uploaded Documents

From time to time, a user of the PLAN CONFIDENCE service may need to upload documents for use of the PLAN CONFIDENCE system. These documents will be uploaded via a web form over a secure HTTPS connection from the user's browser to the PLAN CONFIDENCE web server. The PLAN CONFIDENCE web server will immediately move and encrypt the uploaded document to secure storage utilizing Amazon's AWS S3 service. This service provides the following:

- Enforces that all documents are encrypted
- Handles all the management of the encryption keys
    - ○ Each document is encrypted with a unique key employing strong multi-factor encryption
    - ○ As an additional safeguard, it encrypts the key itself with a master key that is regularly rotated
    - ○ Uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256)

- Durability
    - ○ Redundantly stores documents on multiple devices across multiple facilities in the Amazon S3 region
    - ○ Designed to sustain concurrent device failures by quickly detecting and repairing any lost redundancy
    - ○ When processing a request to store data, the service will redundantly store the document across multiple facilities before indicating success
    - ○ Regularly verifies the integrity of the data using checksums

Access Rights

Information security is the protection of information against accidental or malicious disclosure, modification, or destruction. Information is an important, valuable asset of PLAN CONFIDENCE which must be managed with care. All information has a value to the firm. However, not all of this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorized use.

Formal procedures must control how access to information is granted and determined.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

Definition

Access control rules and procedures are required to regulate who can access PLAN CONFIDENCE information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing PLAN CONFIDENCE information in any format, and on any device.

Risks

On occasion business information may be disclosed or accessed prematurely, accidentally, or unlawfully. Individuals or companies, without the correct authorization and clearance may intentionally or accidentally gain unauthorized access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of the firm and may result in financial loss and an inability to provide necessary services to our customers.

Password Construction

Passwords are the first line of defense for our systems and together with the user ID help to establish that people are who they claim to be.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

Weak and strong passwords

A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Everyone must use strong passwords with a minimum standard of: ·

- At least seven characters
- Contain a mix of alpha and numeric, with at least one digit
- More complex that a single word

Password Protection

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different firm systems.
- Do not use the same password for systems inside and outside of work.

If you become aware, or suspect, that your password has become known to someone else, you must change it immediately and report your concern to a member of the Compliance Committee.

Personal Devices

Personal devices (e.g. smartphones, tablet, or laptops) used to access PLAN CONFIDENCE's system remotely are required to follow the password construction standards defined within this policy. All personal devices must also be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes, maximum. Screens must be locked or logged off when the device is unattended.

PLAN CONFIDENCE does not have the ability to monitor, track or deactivate individual personal devices used by employees to access the firm's system through Amazon Web Services however in cases where access must be removed, complete access to the firm's system can be disabled through Amazon Web Services and/or the Plan Confidence backend administrative site (Management Console and Wizard) immediately.

Access Management

Formal user access control procedures will be documented, implemented, and kept up to date for each application and information system to ensure authorized user access and to prevent unauthorized access. It must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.
- Use multi-factor authentication where possible.

Requests for access to PLAN CONFIDENCE's system must be submitted to PLAN CONFIDENCE through a documented written request and granting access will be documented on the firm's New Hire Checklist. When an employee leaves the firm, their access to the system and data must be suspended immediately. It is the responsibility of the firm to request the suspension of the access rights through Amazon Web Services. Removal of access rights will be documented on the firm's Termination/Resignation Checklist. Changes to access rights during an employee's time of employment due to change in responsibilities, etc. do not require documentation; changes in responsibilities would be discussed as a management team, access would be discussed and the appropriate administrator for the affected applications would then make the changes.

Access Compliance

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.
If any user is found to have breached this policy, they may be subject to disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

Patch Management

Amazon Web Services removes the need for server patching and updates at the firm level. Firm's servers are hosted by Amazon Web Services in their cloud environment therefore Amazon Web Services maintains, updates, and patches the servers within their cloud solutions. Amazon does not automatically apply all updates to the servers. They DO automatically apply security focused patches, but some other updates need us to tell AWS to apply the updates.

PLAN CONFIDENCE takes reasonable steps to select and retain third party service providers capable of maintaining appropriate security measures through discussions with the vendor and conducting reasonable due diligence. During contract negotiations, PLAN CONFIDENCE ensures that each contract contains provisions relating to the protection of clients' personal information and mandates that each vendor represent that they have reasonable safeguards in place to protect accordingly. These representations will be reviewed annually by PLAN CONFIDENCE.

PLAN CONFIDENCE has implemented procedures that restrict access to PLAN CONFIDENCE's systems to active participants and active employees only. If a PLAN CONFIDENCE employee has been terminated, PLAN CONFIDENCE immediately blocks access to physical and electronic documents that may contain client information.

PLAN CONFIDENCE will also deactivate and restrict access to the records of any client that terminates their account in writing or remains 30 days in arrears.

Participants will be responsible for creating their own password. Passwords created must be:

- Seven character minimum
- At least one Upper Case character (A-Z)
- At least on Lower Case character (a-z)
- At least one numeric digit (0-9)
- Case sensitive

Access to the participant's account will be blocked after 3 failed attempts using an incorrect password. The User will have to request Plan Confidence to "unlock" their account and the user will have to reset the password using the link sent to the email address that PLAN

CONFIDENCE has on file or contact support@planconfidence.com or their adviser to reset their password.

Any theft or loss of employee laptops/phones must be reported to PLAN CONFIDENCE immediately.

Each employee of PLAN CONFIDENCE will agree to a “clean desk” policy and all paper items with any client information will be removed and secured when the employee is done working for the day.