Strategic Wealth Partners
Deerfield, IL • 224.632.1600
Milwaukee, WI • 414.359.1000

Your Privacy is Important to SWP!

Data security is a continual concern to individuals and businesses alike. At Strategic Wealth Partners (SWP), we take data security very seriously. SWP has adopted various procedures and policies as it relates to data security, including the following:

Cybersecurity

- SWP requires call-backs to verify third-party fund transfers; including calling the title company for home closing wires to verify wire instructions.
- If a client notifies SWP that their data has been breached, firm procedures include a notification to the entire team to be on heightened alert for any fraudulent activity.
- The firm has adopted procedures to protect nonpublic personal information that is electronically stored or transmitted.
- The Chief Compliance Officer (CCO), or other designated person(s), oversees the selection and retention of third-party service providers. Reasonable steps are taken to select vendors capable of maintaining appropriate safeguards for the data at issue.
- The firm conducts regular tests of its equipment to identify threats, vulnerabilities, etc.
- Firm cybersecurity policies and procedures are available to all employees on the SWP internal file server.
- The firm has adopted procedures governing the use of personal electronic devices for firm business purposes.
- The firm prohibits employees from installing software on company owned equipment without first obtaining approval from management.
- The firm has adopted procedures to promptly eliminate access to all firm networks, devices, and resources in the event an employee resigns or is terminated. Departing employees must return all firm-related equipment and information to the CCO or their designated representative.

Training & Education

- Through periodic blogs and whitepapers, SWP educates clients on recent cybersecurity trends and provides tips to protect data from hackers.
- The firm provides training to employees regarding information security risks and responsibilities no less than annually. Additional training and/or written guidance may also be provided to employees in response to relevant cyber-attacks.

Data Privacy & Security Controls

- The firm has policies and procedures in place for protecting clients' data.
- Client records are retained as needed to comply with applicable retention laws, regulations, and firm record retention policies.
- Asset inventory and asset decommissioning are managed internally, assisted by SWP's external technology firm when necessary.
- Two-factor authentication is required for accessing the firm's network.
- It is firm policy that employee desks are clean of any client information at the end of the workday. Client information is required to be filed away in a locked cabinet when employees leave for the day.
- Access to removable media is controlled by company policy. Removable media is prohibited for non-management employees.
- The firm's privacy policy is emphasized during the onboarding of new employees and reiterated throughout the organization via regular team meetings and annual compliance review meetings.
- For more information, please see SWP's Privacy Policy available on the Strategic Wealth Partners website.

Encryption

- Company computers are encrypted using Microsoft Bitlocker encryption.
- Email encryption is required when emailing personally identifiable information (PII) including account numbers, passwords, or other personal information.
- The firm's data is encrypted through the use of a hosted environment structure. Per firm policies, no client data is stored on local computers.
- All firm issued desktop and laptop computers are installed with enterprise anti-virus software which is monitored by an external information technology firm.

Vendor Security

- The firm has implemented policies and procedures to review vendors' technology and security risks. Through this process, the firm identifies vendor control gaps and other deemed risks as specified by SWP compliance.
- New vendors are required to complete a vendor due diligence assessment questionnaire before the use of the vendor is authorized.
- In addition to the questionnaire, SWP requests that vendors provide a certificate of insurance, privacy statement, report on controls (such as an SSAE 16 SOC I), and business continuity plan.
- Ongoing vendor due diligence assessments are conducted annually and reviewed by management.

Mobile Security

- In order for employees to add company email to their personal mobile device, there are certain policies that must be met: (1) the device must be encrypted and (2) a passcode or equivalent authentication must be required when unlocking the phone.
- In the case of a lost or stolen phone, company email access is removed from the mobile device.

Physical Security

- All offices require a code to enter before and after normal business hours.
- Building staff (cleaners) have a unique code.
- All vendors visiting the office must sign in at the front desk and show identification.
- It is the firm's policy that all documents containing sensitive information are locked up overnight. Nothing is to be left on an employee's desk. Random audits are conducted in each location.
- The firm utilizes a NAID certified shredding company to securely shred all documentation containing sensitive information.

Date Published: 09/23/2019