Illuminating your family's path to a brighter financial future.

Carrie Houchins-Witt Tax & Financial Services LLC
1303 5th Street Suite 207
Coralville IA 52241
www.houchinswitt.com
319.359.0439

SECURITY POLICIES & PROCEDURES

Carrie Houchins-Witt Tax & Financial Services is serious about securing clients' personal data. Carrie does not disclose any non-public personal information about clients (current or former) to anyone, except as instructed to do so by such clients or as required by law. Carrie restricts access to non-public personal information to those necessary to prepare tax returns and financial plans. Carrie maintains electronic, physical and procedural safeguards to guard clients' non-public personal information. As such, Carrie practices the following security measures to ensure both the electronic and physical security of personal data of her clients:

ELECTRONIC SECURITY

- All computer and all electronic client files are encrypted with either the **Symantec Endpoint Encryption** product or the **Microsoft Windows BitLocker Drive Encryption** product. This means that if an unauthorized party manages to access the encrypted data, all they will find is streams of unintelligent, alphanumeric characters that cannot be deciphered.

- In order to electronically share and transmit sensitive documents with clients, the **SecureFilePro** product is employed rather than transmitting an unsecure attachment in an email message or by fax. This product allows Carrie and her clients to easily upload and access electronic documents through a secure web portal, accessible through Carrie's website. All transmissions are secured with 256-bit SSL encryption, and files are encrypted at rest on the server. At all times, clients can view and access only their own documents.
- Anti-virus, anti-spyware and anti-malware software such as **Microsoft Security Essentials / Windows Defender** and **Malwarebytes Anti-Malware** are frequently scheduled to conduct regular full-system scans of all computer(s) to ensure any virus, spyware or malware is identified and neutralized.
- Multiple layers (hardware and software) of **firewall technology** are employed to identify and manage any potential malicious content or applications. Carrie's wireless router contains firewall technology as part of its hardware, and Windows Firewall is enabled on all systems.

- All wireless routers **encrypt transmission of data using the industry's highest security standard (WPA2+AES)**. This means that hackers will be unable to decipher any information if it is intercepted during the wireless transmission from the computer to the router. In addition, access to Carrie's router is password protected, and her wireless network's broadcasted name (SSID) is not specific to her business. The password is maintained as business proprietary information.
- In order to back-up clients' data and files, Carrie's business process employs the **secure, cloud-based Carbonite product**. All backed-up clients' information is encrypted using 128-bit Blowfish encryption. Data is then transmitted to one of Carbonite's data centers using a Secure Socket Layer (SSL) and protected by multiple levels of on-site, physical and electronic security, including 24 hour security, limited personnel access through the use of biometric scanning, passwords and electronic key cards, temperature control, uninterrupted power supply and back-up generators in case of power failure.
- Carrie's business process engages the "automatic update" feature for Windows and other applications on her computer(s). This results in security patches and updates being installed expeditiously thus avoiding potential malware infection.

PHYSICAL SECURITY

- All office space is protected by two layers of locking, secure doors, including the entrance to the building and her office door.
- All file cabinets lock and are secured at the end of each business day.

PROCEDURAL SECURITY

- Sensitive, personal information will never be transmitted as an attachment to an email or within the body of an email. Carrie encourages all of her clients to do the same and only utilize the aforementioned SecureFilePro (see Electronic Security section) for transmission of this kind of sensitive data.
- Passwords for access to all encrypted information or any router are considered business confidential and proprietary information. As such it is only available to trusted personnel in Carrie's business.
- Carrie requires the use of Power of Attorney documents permitting the disclosure of clients' information to third parties.
- Carrie strives for a paperless work environment, which aides in the security of client information. Any hard-copy client documents that are not returned to the client or not kept for Carrie's files are shredded.
- Any client documents that are returned by Carrie by mail are sent "priority mail" through the US Postal Service (USPS), with tracking information in the event the package is lost by USPS.