



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

319.358.2854

SECURITY POLICIES & PROCEDURES

Carrie Houchins-Witt Tax & Financial Services LLC 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 unintelligible, alphanumeric characters that cannot be deciphered.
- In order to keep office computers up-to-date, protected and backed-up, **Computer Solutions (a third-party IT vendor located in Iowa City, Iowa) provides Windows patch management, anti-virus and anti-malware products, and daily managed cloud back-up.**
 - Through Computer Solutions, the Managed Pro PC with Anti-Virus + Anti-Malware product is employed and monitored on office computers. Specifically, Windows/Microsoft patch updates are scheduled and installed to ensure each office computer remains upgraded and secure. The Managed Anti-Virus + Anti-Malware features include regularly scheduled scans at noontime and after-hours, with any issues/concerns reported to Computer Solutions through an end-of-day summary.
 - Through Computer Solutions, the Managed Cloud Back-up product (through IDrive) allows daily back-up of each office computer's files to an encrypted cloud account. If back-up fails, Computer Solutions is notified and performs the appropriate remedy. IDrive uses industry standard 256-bit AES encryption on transfer and storage. Data is

stored in encrypted form at IDrive data centers, which are protected through 24/7 on-site security, HVAC temperature control systems, and seismically braced racks.

- 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.
- 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 office work computers and printers are hardwired to the internal office network. For the few instances where wireless devices are utilized, the office router **encrypts 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. Passwords are maintained as business proprietary information.

PHYSICAL SECURITY

- Carrie's office is protected 24/7 by a professionally installed and monitored alarm system. Any unauthorized entry into her office will trigger a siren as well as a call to the local police department for immediate response to the security breach.
- In addition to the office alarm system, all office space is protected by two layers of locking, secure doors, including the entrance to the office suite and each office within the suite.
- 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. With respect to hard copies of client documents, Carrie's record retention policy calls for the electronic scanning and archiving of documents older than one year, and then the shredding of said documents.
- While client documents are rarely removed from the office, on such occasions, Carrie keeps all documents securely on her person and returns them to the office the same or next day. Only Carrie removes documents from the office (other staff are prohibited from do so).
- When office computers become obsolete, the hard drives are personally removed from the computers by Carrie's IT staff person and physically destroyed.
- While a data breach of Carrie's systems has never occurred, if such an incident were to take place, Carrie would notify all clients impacted by the loss or theft of personal records. Carrie would work with her data breach insurer to ensure that notifications of such loss/theft were sent to all affected clients and would work with the insurer to provide such clients with identify theft protection.
- Any sensitive client documents that are returned by Carrie by mail are sent through the US Postal Service (USPS) with tracking information to ensure the package reaches your home.