KEVIN WENIG ▪ CPA
A LIMITED LIABILITY COMPANY

WORK FROM HOME POLICIES

The following *Work From Home* ("WFH") policies are designed to maintain security, professionalism and helps us to work seamlessly with each other and our clients.

SECURITY:
You must keep the most up to date operating system (OS) on your computer, whether it's your own computer or it's provided to you. Keeping software up to date is an absolute condition of employment at KWCPA. Please set it to "update automatically".

You must use a unique password on both your home router and your computer that you don't use anywhere else. If practical, please create a separate login on your home router for your work computer.

Computers must have a login password, lock when not in use for more than ten minutes and go to sleep/shut down overnight if you don't turn it off manually.

You are expected to use dual authentication anywhere you can, most notably with Dropbox and email.

Password protecting a .pdf is a weak and easily breakable security measure. Instead, always use Dropbox Transfer with a password and an expiration date when sending sensitive data outside of our organization. Passwords can be texted or given verbally to our clients. Never state the password in an email or give a hint like "use the last four digits of your Social Security number." This is not secure.

You must set your hard drive to be encrypted.

Enable Dropbox Smart Sync. Doing so saves space, speeds up your computer and physically stores less information on your hard drive.

Tether your laptop to your mobile phone when away from a trusted Wi-Fi source, like your own home. Never use WI-FI offered at coffee shops, train stations, airports, etc.

You will be provided a backup drive that must be connected to your computer. This not only provides a backup but will enable you to quickly start up a new computer if yours is "bricked" because of ransomware.

Nothing is to be stored on your desktop or flash drives. Dropbox is backed up, has built in security features and is also shared with the rest of the team.

All passwords must be entered in LastPass. Set it to open at login.

Please verify client & vendor ACH/Wire credentials over the phone before making or accepting a payment. This is vital when initially setting up their banking information and when changes are requested.

Please only go to reputable websites on company owned machines, no illegal or in appropriate downloads for any reason. You will accept responsibility for viruses and other issues related to questionable websites.

Children, friends, spouses are never to use your computer. You are free to use it for personal purposes, but no one else should have access to it considering the amount and types of sensitive data we store in it.

The expectation is that wherever you are, you have a suitable workspace with business class internet and a setting appropriate to perform your job and communicate just as efficiently as you would in an office setting.

Above all - use common sense. Don't leave papers out, discuss clients in front of kids/friends, etc.

Please let me know if you need help with these or any other issues you may have or if you have questions.

ADMINISTRATIVE

Use email aliases when appropriate:

- tax@wenigcpa.com, which goes to those who are in our tax and accounting department
- finance@wenigcpa.com, goes to all those working on "FOP" clients
- team@wenigcpa.com – sent to all full-time employees
- all@wenigcpa.com – firm-wide, including contractors, hourly and part-time employees

Check the mail folder/email everyday.

Shredding; Please shred all sensitive documents or bring it to Staples/UPS Store. Better yet, keep it digital and don't use paper at all. Envelopes don't need to be shredded. Only those papers with two or more of the following need to be shredded:

- Names
- Financial information
- Social Security numbers
- Easily identifiable financial information

Printed tax returns should always be shredded.

Cross-subscribe to Calendars so people can schedule time with you and you with others.

KWCPA will provide specific items you may need exclusively for work. i.e., scanner, keyboard, mouse, headset/speaker, etc.

We pay $15 per paycheck to cover direct costs of working from home. This includes internet, electricity, small incidental supplies, use of your mobile phone, shredding, etc.

APPEARANCE AND WORKSPACE

Video etiquette – it's becoming more acceptable and even preferred to use video vs. using the phone as a more engaging way to communicate. Studies show people overwhelmingly believe it's '**rude'** to watch others eat and '**distracting'** when someone is drinking. Please avoid both, especially when talking with clients.

Dress is business casual like you would dress in an office; you are expected to be clean shaven, no hats or sweatshirts, t-shirts, etc. Although you are working remotely, we are still a CPA firm and clients expect a level of professionalism that does not exist when wearing casual clothing. Clients may (and often do) present themselves with casual attire but that is not an invitation to follow suit. Calls within our company can be less formal.

Have an uncluttered desk space if visible and be aware of your background when on video calls.

Be aware that people are reluctant to discuss financial and personal items with you when they see other people within earshot of you or passing through your workspace. It should be private, quiet and free of distractions for our clients.

We need to give the appearance that confidentially, security and organization can be maintained wherever you are.

WFH means a certain amount of flexibility is acceptable. You have unlimited PTO and flex hours (within reason) but everyone has to put in 1,800 hours each year (tax staff are 2,000). You are expected to be available for client needs during business hours.

Planned time off and time away from your desk should be entered in your calendar so others can schedule time with you.

As was the case when we were in an office, March 15, April 15, September 15 and October 15 are “All Hands on Deck” days and everyone is expected to be available all day without exception.

Our clients are mostly on the East Coast. For this reason, we will use Eastern Standard Time as the company standard.

Acknowledged:

_____	_____	_____
Print name	Signature	Date

Acceptable Use Policy

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at KWCPA. These rules are in place to protect the employee and KWCPA. Inappropriate use exposes to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct business or interact with our internal business systems, whether owned or leased by KWCPA, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at KWCPA and its subsidiaries and divisions are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at KWCPA, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by KWCPA.

General Use and Ownership

KWCPA proprietary information stored on electronic and computing devices whether owned or leased by KWCPA, the employee or a third party, remains the sole property of KWCPA. You must ensure through legal or technical means that proprietary information is protected in accordance with data protection standards.

You have a responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.

You may access, use or share proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/ Intranet/Extranet systems. In the absence of such policies, employees should consult their supervisor or manager.

For security, network maintenance, and client continuity purposes, authorized individuals may monitor equipment, systems, network traffic, emails and/or chat messages at any time.

KWCPA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

All mobile and computing devices that connect to the internal network(s) and systems must have the approval of the system administrator.

System level and user-level passwords must comply with IRS guidelines for passwords. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

Each employee/user shall have their own account login and passwords. Passwords shall not be shared between different accounts.

Employees must use extreme caution when opening e-mail attachments; avoid opening those received from unknown senders, which may contain malware.

All local data must be regularly backed up to the hard drive you have been provided.

The system owner/administrator must be notified immediately of any breach of data security or damage to the physical security of the office.

The system owner/administrator shall devise a physical security policy for the company. It should be kept on file with this policy document.

Unacceptable Use

Under no circumstances is an employee of authorized to engage in any activity that is considered “high risk” or illegal under local, state, federal or international law while utilizing KWCPA-owned resources.

Other activities that are expressly forbidden:

Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)

Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

Revealing a client's Social Security number or other Personally Identifiable Information (such as bank account numbers) to anyone other than another employee, or for any purpose other than preparing a tax return or similar work product. This prohibition includes temporary employees and contract employees such as IT technicians.

Using a computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

Education and Training

A copy of this security policy will be provided each employee and must be "recertified" at least annually.

I, the undersigned, recognize that failure to adhere to the KWCPA Acceptable Use Policy could lead to termination of employment:

Acknowledged:

_____	_____	_____
Print name	Signature	Date