Fairoaks IT
Cybersecurity | AI Advisory | Managed IT | Cloud

2026 edition

Before You Hire (or Fire) Your IT Company

The Accounting Firm's Q&A Guide

Straight answers for partners, owners and office managers at CPA, accounting and tax firms, plus five tools you can put to work before tax season.

Soteria Award winner
Most Trusted MSP in North America

Prepared by **Tom Crossley, Founder and President, Fairoaks IT**	Established **1991, independent and owner-led**
Serving **Eastern Massachusetts, Rhode Island and the Charlotte, NC area**	Offices **Franklin, MA and Belmont, NC**

What's inside

The 2-minute scorecard	3
Is it time to fire your IT company?	4
Tax season and uptime	5
IRS and FTC requirements	7
Security, fraud and client data	10
Cost, contracts and switching	12
10 questions to ask before you sign	15
Tool 1: WISP outline checklist	16
Tool 2: Pre-tax-season IT checklist	17
Tool 3: Client document policy starter	18
Tool 4: Data theft response checklist	19
Tool 5: Seasonal staff checklist	20
What happens in an assessment	21
About Fairoaks IT	22

From the desk of Tom Crossley

Accounting firms have been part of Fairoaks IT since I started the company in 1991, and some have been with us for decades. Over those years I've watched the job get harder. Returns moved online. Clients started emailing Social Security numbers. Criminals started targeting tax professionals by name. And the IRS and FTC started expecting a written plan for all of it.

When your technology works, nobody notices. When it doesn't, it shows up in March: a slow server, a locked-out partner, a "new client" email that wasn't a client at all.

The most common story I hear from accounting firms isn't about a hacker. It's about a partner who is paying an IT company and still managing every problem personally, usually at nine at night in tax season.

So I wrote this guide to give you straight answers. Whether you're hiring your first IT company, thinking about firing the one you have, or just want to know where you stand, you'll find:

- a 2-minute scorecard to see where your IT stands today
- the warning signs that it's time to make a change
- plain-English answers about tax season, the IRS and the FTC Safeguards Rule
- 10 questions to ask any IT company before you sign
- five tools you can copy and use before tax season

No scare tactics and no jargon. If something in here raises a question, call us. If we're not the right fit for you, I'll tell you.



Tom Crossley
Founder and President, Fairoaks IT

Start here

The 2-minute scorecard: is your IT built for an accounting firm?

Check yes only if you're sure. "I think so" counts as no. That isn't us being tough; it's how the FTC or an insurance carrier will see it if something goes wrong.

1	When someone calls for IT help, a real person starts on it within minutes, not hours, even in tax season.	☐ Yes	☐ No
2	Your written information security plan exists, matches how the firm works today, and was reviewed in the last year.	☐ Yes	☐ No
3	You know who your firm's Qualified Individual is, and that person gets regular security reports.	☐ Yes	☐ No
4	Every email account and every remote login, including the partners', uses multi-factor authentication.	☐ Yes	☐ No
5	Clients send documents through a secure portal, not regular email.	☐ Yes	☐ No
6	Client information on laptops and in transit is encrypted.	☐ Yes	☐ No
7	Backups of client files and tax software data are stored where ransomware can't reach them, and were test-restored in the last 90 days.	☐ Yes	☐ No
8	Your security is tested: ongoing monitoring, plus penetration tests and vulnerability assessments on schedule.	☐ Yes	☐ No
9	Seasonal and departing staff lose access the day they leave, using a checklist.	☐ Yes	☐ No
10	Staff know how to spot a "new client" phishing email and verify new clients by phone.	☐ Yes	☐ No
11	You have a written plan for what to do if client data is stolen, including who to call at the IRS.	☐ Yes	☐ No
12	Your IT costs are predictable, and you know exactly what is and isn't included.	☐ Yes	☐ No

11 to 12 yes

You're in good shape. Use the rest of this guide to keep it that way.

8 to 10 yes

A solid foundation with real gaps. Fix the no's before tax season, starting with your WISP, MFA and backups.

5 to 7 yes

You're carrying more risk than you probably realize. One bad email or failed server could cost you a season.

0 to 4 yes

Your IT is running on luck. Let's talk before the luck runs out.

The “fire” part

Is it time to fire your IT company? Eight warning signs

Plenty of firms already pay for IT support and still aren’t getting it. If three or more of these sound familiar, it’s time for a serious conversation, either with your current provider or with a new one.

1

You’re still chasing them.

You pay for IT support, and you’re still the one following up, escalating and checking whether anything got done.

2

The same problems keep coming back.

They fix the symptom and move on. A week later it’s back, and nobody has looked for the cause.

3

You have to explain your tax software.

If you’ve had to explain what UltraTax CS, Lacerte or CCH Axcess is, they’re learning on your dime.

4

Nobody can tell you if your backups work.

Ask when they last did a test restore of your client files. A vague answer is the answer.

5

They disappear in tax season.

Response times stretch out exactly when you need them most, between February and April.

6

They go quiet on your WISP.

The FTC Safeguards Rule or PTIN renewal comes up, and suddenly nobody has an answer.

7

You only hear from them when something breaks.

Or when the invoice shows up. No planning, no reviews, no recommendations until there’s an emergency.

8

Everything lives in their head.

If you asked for your admin passwords and network documentation today, could you get them? If not, they control your IT, not you.

> **Worried about switching during a busy year?** The answer is timing. Page 14 walks through what a clean, off-season switch looks like.

Chapter 1

Tax season and uptime

Tax season is when IT problems cost the most. This chapter covers getting ready in the fall, staying up in the spring, and keeping remote and seasonal staff productive and secure.

How do we get our IT ready before tax season?

Start in the fall, while there's still time to fix what you find:

- Install tax software updates and confirm licenses and versions
- Replace computers that won't make it through the season
- Test that backups of client files and tax data actually restore
- Review who has access to what, and remove anyone who has left
- Turn on multi-factor authentication everywhere it's missing
- Set up seasonal staff in advance, not on their first morning
- Update your written information security plan

The pre-tax-season checklist on **page 17** puts all of it on one page.

What happens if our systems go down in March or April?

With the right preparation, a bad hour instead of a lost week. That takes backups stored where ransomware can't reach them and tested regularly, a recovery plan that says how fast your tax software and client files come back, and support that starts fast.

At Fairoaks IT, our average time to start on a support issue is under 12 minutes, with live support during business hours and after-hours support available. Without that preparation, an outage in April can mean missed deadlines, extensions and clients calling to ask what happened.

Chapter 1, continued

Tax season and uptime

Quick win

Schedule big IT changes for May through September. Nothing new should go live in tax season.

How can remote and seasonal staff work securely?

Give them company-managed laptops or a secure hosted environment instead of personal computers, require multi-factor authentication on every login, keep client files in your portal or file system rather than on home computers, and use remote access you can turn off the day the season ends. The checklist on **page 20** covers both arrival and departure.

Should our tax software run on a server, in the cloud or hosted?

It depends on your software and how your team works. Cloud products like CCH Axcess and ProConnect run in the vendor's cloud. Desktop products like UltraTax CS, Lacerte, ProSeries, Drake and QuickBooks Desktop can run on a well-maintained office server, or in a secure hosted environment your team reaches remotely, which makes remote work much easier.

We lay out the options, costs and security trade-offs side by side before anything moves.

What should happen when someone needs help late in the season?

They should know exactly who to call. For firms that work late during the season, we plan ahead: monitoring that catches problems before morning, a clear process for urgent after-hours issues, and making sure the systems you depend on are updated and tested before the season starts.

Chapter 2

IRS and FTC requirements

The IRS and FTC expect accounting firms to protect client data the way a financial institution would, in writing. This chapter covers what the rules require and what they don't.

Does the FTC Safeguards Rule apply to our firm?

Almost certainly. The FTC treats tax preparation firms as financial institutions, so the Safeguards Rule applies whether you're a sole practitioner or a large firm. It requires:

- A written information security program
- A Qualified Individual who oversees it
- A risk assessment the program is built on
- Safeguards including multi-factor authentication, encryption, access controls and secure disposal
- Testing and monitoring, staff training and vendor oversight
- An incident response plan and breach notification to the FTC

What is a WISP, and what goes in one?

A written information security plan, or WISP, documents how your firm protects client information: who's responsible, what risks you face, the safeguards in place, how staff are trained, how vendors are overseen and what you'll do after a breach. The IRS expects every paid preparer to have one.

IRS Publication 5708 provides a sample template, but a plan only helps if it reflects how your firm actually works and is kept current. The outline checklist on **page 16** shows what yours should cover.

30 days

The deadline to notify the FTC after discovering a breach of unencrypted information about 500 or more consumers.

What does PTIN renewal ask about data security?

PTIN renewal opens in mid-October each year, and PTINs expire on December 31. The renewal form, Form W-12, includes a question about the requirement for paid preparers to have a written information security plan. The requirement itself is real, so renewal season is a good time to make sure your plan exists and reflects how your firm works today.

When must we notify the FTC about a breach?

Since May 13, 2024, firms must notify the FTC as soon as possible, and no later than 30 days after discovery, when unencrypted information about 500 or more consumers is acquired without authorization. The count is consumers, not households, so spouses and dependents count. State laws, client notices and IRS reporting can apply too.

What is a Qualified Individual?

The person the Safeguards Rule requires to oversee, implement and enforce your security program. An outside provider can fill the role, but your firm stays responsible and must name a senior person of its own to oversee them. At Fairoaks IT, we support the Qualified Individual you designate with the reports, evidence and recommendations they need.

IRS and FTC requirements

Worth knowing

Your WISP has to change when your firm does: a new office, new software, a merger or a new way of working.

What testing does the rule require?

Either continuous monitoring of your systems, or an annual penetration test plus vulnerability assessments at least every six months, along with additional testing after major changes. Keep the results: testing only counts if you can show it happened and that findings were fixed. We provide penetration testing and vulnerability assessments for accounting firms.

Do smaller firms get any relief?

Some. Firms that maintain information on fewer than 5,000 consumers are exempt from a few requirements, including the written risk assessment, the written incident response plan, annual reporting to leadership and certain testing requirements. They still need a written program, a Qualified Individual, multi-factor authentication, encryption, secure disposal, training and breach notification.

What are IRS Publications 4557 and 5708?

Publication 4557, Safeguarding Taxpayer Data, is the IRS guide to protecting client information: security basics, recognizing data theft and what to do after it. Publication 5708 walks tax professionals through creating a written information security plan. Both are free from the IRS and a good starting point, but neither replaces actually putting the safeguards in place.

Chapter 3

Security, fraud and client data

Accounting firms are targeted because of what they hold. This chapter covers how criminals get in, how to keep client data out of their hands, and what to do if they succeed.

Why are tax professionals targeted?

Because your files hold exactly what criminals want: Social Security numbers, birth dates, bank account numbers and tax data they can use to file fraudulent returns or open accounts. Firms also handle a huge volume of email and attachments from people they don't know well, especially in tax season, which makes phishing easier.

The defense is layered: multi-factor authentication, email filtering, endpoint protection, encrypted file exchange, tested backups and trained staff. At Fairoaks IT, security updates, endpoint protection and 24/7 monitoring come standard. Most of our plans add staff training and phishing simulations, and our advanced security option adds a 24/7 security operations center.

What do "new client" scams look like?

An email arrives from someone who says they need a return prepared, often mentioning a referral, with a link or attachment that supposedly holds their tax documents. Opening it can install malware that steals passwords or gives criminals remote access. The IRS and its Security Summit partners warn tax professionals about these scams every year. Watch for:

- A new client you've never spoken to who wants to send documents right away
- Links to download files, or attachments you have to enable to view
- Pressure to act quickly, or a reply-to address that doesn't match the sender

Verify new clients by phone, using a number you look up yourself, and have them use your portal.

Security, fraud and client data

Software we support

CCH Axcess, CCH ProSystem fx, UltraTax CS, Lacerte, ProConnect, ProSeries, Drake, QuickBooks Desktop and Online, SmartVault, ShareFile, Canopy, Karbon, TaxDome and Microsoft 365.

How should we exchange documents with clients?

Use a client portal, not email. Portals encrypt files, track who downloaded what, and keep Social Security numbers out of inboxes. Turn on multi-factor authentication, ask clients to use the portal every time, and make it easy for them. When something must go by email, encrypt it. The policy starter on **page 18** gives you the wording.

What should we do if client data is stolen?

Act fast and follow your written plan. Contact your IT provider and your cyber insurance carrier immediately, preserve evidence, and contact your IRS Stakeholder Liaison so the IRS can help protect your clients' accounts. Notify the states where you prepare returns and contact law enforcement. If unencrypted information about 500 or more consumers was taken, notify the FTC within 30 days, and check state breach laws for client notices. The checklist on **page 19** lays it out hour by hour.

Can staff use AI tools with client data?

Not with free or personal AI accounts. Client tax data shouldn't go into tools that aren't approved for it, and doing so can conflict with your WISP. Business-grade tools, including options within Microsoft 365, can be set up with the right protections. Name the approved tools in writing and list what never goes in.

Chapter 4

Cost, contracts and switching

This is where most IT relationships go right or wrong. This chapter covers how IT companies charge, what to watch for in a contract and how to switch without touching tax season.

How do IT companies charge, and which model puts the risk on you?

There are three common ways:

- **Time and materials (break-fix):** you pay by the hour when something breaks. It looks cheap until a bad March. The provider makes more money when your systems have more problems, so nobody is paid to prevent them.
- **Managed services:** a predictable monthly fee, usually per user or per device, covering support, maintenance and monitoring. The provider does better when your systems run well.
- **Software vendor support:** help with one application only. Useful, but it stops at the edge of their software.

For a firm that can't afford a lost day in tax season, managed services almost always makes the most sense. Our IT Buyer's Guide covers each model in detail at **fairoaksit.com/itbuyersguide**.

What should be included in the monthly fee, and what's usually extra?

Every provider draws the line in a different place, so get it in writing. Monthly plans typically cover support for your users, monitoring and maintenance, security tools, backup management and Microsoft 365 administration. Hardware, software licenses and tax software subscriptions are almost always extra, and projects like a server replacement, a move to a hosted environment, or WISP and penetration testing work are usually quoted separately.

At Fairoaks IT, our plans cover labor, hardware and software are billed separately, and we explain every cost up front.

Cost, contracts and switching

Get it in writing

Your passwords, documentation and data belong to you, no matter who your IT provider is.

What contract terms should make us nervous?

- **Vague scope:** "unlimited support" with no definition of what's covered
- **Buried exclusions:** especially onsite visits, after-hours work and anything labeled a "project"
- **Open-ended project billing:** hourly work with no estimate or cap
- **No way out:** long terms with no remedy if service is poor
- **Unclear ownership:** no written answer on who owns your passwords, documentation and data if you leave

That last one matters most. Your admin passwords, network documentation and data belong to you. Any provider who hesitates to say so in writing is telling you something.

How long should an IT agreement be, and what if it isn't working?

Multi-year agreements are common, and they can work in your favor: they lock in your rate and give the provider reason to invest in your environment.

What matters is what happens if things aren't working. Ask every provider two questions: what happens if you don't deliver, and how are price increases handled? Get both answers in writing. Ours are spelled out in our agreement, and we'll walk you through every page before you sign.

Before you sign

Ask every provider to walk you through their onboarding plan, and when it would happen.

How do we switch IT providers without disrupting tax season?

Switch in the off-season. The best window is late spring through early fall, away from your filing deadlines. A clean switch looks like this:

1. Discovery before anything changes: every system, password, license and vendor documented, including your tax software, client portal and remote access
2. A coordinated handoff from your current provider. Nobody flips a switch on a Friday afternoon.
3. The biggest risks fixed first, like backups and multi-factor authentication
4. One named point of contact and weekly check-ins until onboarding is done
5. Your WISP updated to reflect the new provider and setup

If a provider can't walk you through their onboarding plan before you sign, keep looking.

Our office manager handles IT. Should we hire an IT person instead?

For most firms, one internal hire is the riskier choice. One person can't be an expert in servers, security, tax software, client portals and compliance at once, and they take vacations and sick days. When they leave, what they know leaves with them.

If you already have someone good, the best answer may be both. Co-managed IT gives them a full team behind them, without replacing them.

The "hire" part

10 questions to ask any IT company before you sign

Bring these to every meeting. The answers tell you more than any proposal, and a good provider will be glad you asked.

1 How fast does a real person start on an issue, including in tax season?

A good answer: A specific average they track and report. Ours is under 12 minutes.

2 What isn't included in the monthly fee?

A good answer: A written list of exclusions, offered without hesitation.

3 Which tax and accounting software do you support today?

A good answer: Names you recognize, like CCH Axcess, UltraTax CS, Lacerte or Drake, without you having to explain them.

4 Can you help us write and maintain our WISP?

A good answer: Yes, with a plan built around how your firm actually works, not a generic template.

5 How will you support our Qualified Individual?

A good answer: Regular reports, evidence and recommendations, with your firm still in charge.

6 What security testing do you provide?

A good answer: Ongoing monitoring, plus penetration testing and vulnerability assessments on a schedule that meets the FTC Safeguards Rule.

7 When did you last test-restore a client's backup?

A good answer: A recent date and what they restored. Not "the backups run every night."

8 How will you onboard us without disrupting tax season?

A good answer: A documented plan scheduled in the off-season, with a point of contact and regular check-ins.

9 If we leave, do we get all our passwords, documentation and data?

A good answer: "Yes, it's yours," and they'll put it in writing.

10 What happens if you don't deliver, and can I talk to an accounting firm you support?

A good answer: A clear, written answer, and references from firms like yours.

How we answer them: under 12 minutes on average to start on an issue, live support during business hours with after-hours support available, the software list on **page 11**, help with your WISP and risk assessment, penetration testing and vulnerability assessments, and an agreement that spells out what's included before you sign.

Tool 1

WISP outline checklist

Print and use

Use this to check an existing plan or start a new one. IRS Publication 5708 includes a sample template you can build on. Every box should point to something written down.

Firm	Qualified Individual	Last reviewed	Next review

Ownership

- [ ] The Qualified Individual is named, with a senior person overseeing them
- [ ] Other security responsibilities are assigned in writing

Risk assessment

- [ ] Client information is listed: what you collect, where it lives, who can reach it
- [ ] Risks are identified, with how each one is handled
- [ ] A date is set to reassess

Safeguards

- [ ] Multi-factor authentication on every system with client information
- [ ] Encryption at rest and in transit
- [ ] Access limited to the people who need it
- [ ] Secure disposal of old records and devices

Testing and people

- [ ] Monitoring, or penetration tests and vulnerability assessments, on a schedule
- [ ] Staff training, including phishing and "new client" scams
- [ ] Vendors listed, with security requirements in their contracts

Incident response

- [ ] A written response plan with roles
- [ ] Contacts: IRS Stakeholder Liaison, insurer, IT provider, attorney
- [ ] FTC notification steps for breaches involving 500 or more consumers

Upkeep

- [ ] Reviewed at least once a year and after major changes
- [ ] Annual report to firm leadership (required at 5,000 or more consumers)

Tool 2

Pre-tax-season IT checklist

Print and use

Work through this between October and early January. Anything you find now is far cheaper to fix than anything you find in March.

October and November

- [ ] Renew your PTIN and confirm your written information security plan is current
- [ ] Confirm tax software licenses, versions and update schedules
- [ ] Replace computers that won't make it through the season
- [ ] Test-restore backups of client files and tax software data
- [ ] Review user accounts: remove anyone who left and confirm access levels
- [ ] Turn on multi-factor authentication everywhere it's missing

December

- [ ] Set up seasonal staff accounts, laptops and remote access in advance
- [ ] Run phishing training focused on "new client" scams
- [ ] Confirm the client portal works, and remind clients to use it
- [ ] Check internet capacity and battery backups for the server and network
- [ ] Review cyber insurance requirements before your renewal

First week of January

- [ ] Install final tax software updates and test e-file
- [ ] Make sure IRS e-Services and tax software logins use strong, unique passwords and MFA
- [ ] Post the IT support number at every desk

Tool 3

Secure client document policy starter

Copy and use

Fill in the blanks, share it with every partner and staff member, and add it to your WISP.

_____ Client Document Policy

1. We accept client documents through our secure portal, _____, or in person.
2. We never ask clients to email Social Security numbers, bank account numbers or tax documents, and staff don't send them by regular email.
3. If something must be sent electronically outside the portal, we use encrypted email.
4. New clients are verified by phone, using a number we look up ourselves, before we open their documents or links.
5. Staff don't open unexpected attachments or links from new or unknown senders; they forward them to _____.
6. Client files are stored only in _____, never on personal devices or personal cloud accounts.
7. We keep client files for _____ years, then delete or destroy them securely.

_____ _____

Approved by Date

What to tell clients: "To protect your information, please upload your documents through our secure portal. We'll never ask you to email your Social Security number or bank details."

Tool 4

Data theft response checklist

Keep a copy offline

Fill in the contacts now and keep a printed copy somewhere you can reach if your systems are down. This is a starting point, not legal advice; your attorney has the final word.

Incident lead	IT provider phone	Insurance carrier phone	Attorney phone

First hour

- [ ] Disconnect affected computers from the network, but leave them powered on
- [ ] Call your IT provider
- [ ] Call your cyber insurance carrier before hiring any outside help
- [ ] Start a written log of what happened, when, and who did what

First day

- [ ] Contact your IRS Stakeholder Liaison
- [ ] Change passwords and confirm MFA on email, tax software and IRS e-Services
- [ ] Call your attorney and contact law enforcement

First week

- [ ] Notify the states where you prepare returns (the IRS data theft guidance explains how)
- [ ] Determine whose information was involved and whether it was encrypted

Within 30 days

- [ ] If unencrypted information about 500 or more consumers was taken, notify the FTC through its online form
- [ ] Notify affected clients and state authorities as each state's breach law requires
- [ ] Update your WISP with what you learned

Tool 5

Seasonal staff onboarding and offboarding checklist

Print and use

Use one copy per person. Seasonal access that lingers into summer is one of the easiest ways in.

Name	Role	Start date	Last day

Before day one

- [ ] Create accounts with multi-factor authentication turned on
- [ ] Provide a company laptop or hosted access, never a personal computer
- [ ] Grant only the tax software, portal and e-file permissions the role needs
- [ ] Have them read and sign the WISP and client document policy
- [ ] Complete phishing training before their first login

On the last day

- [ ] Disable their accounts and sign them out of every session
- [ ] Remove tax software, e-file and client portal access
- [ ] Remove company email and data from personal phones
- [ ] Collect laptops, keys, badges and security tokens
- [ ] Move any client files they kept into firm storage
- [ ] File this checklist with your WISP records

Next step

What happens in a Fairoaks IT assessment

We look at your technology the way you'd look at a client's books: all of it, with a written report at the end. It starts with a discovery call.

> **Schedule a discovery call**
> fairoaksit.com/discoverycall

What we review

- Your servers or hosted environment
- Tax and accounting software setup
- Client portal and document exchange
- Microsoft 365 and email security
- Backups, and whether they can actually be restored
- Security tools and updates
- Your WISP, risk assessment and testing records
- Cyber insurance requirements

What you get

A plain-English report on what's working, what's at risk and what to fix first, with quick wins called out and monthly support kept separate from one-time projects. No scare tactics, just facts. If we're not the right fit, we'll tell you.

What you can count on

Help in minutes, not hours. Our average time to start on a support issue is under 12 minutes, with live support during business hours and after-hours support available.

No surprises. Before you sign, you'll know exactly what's included, what isn't and how every cost works. It's all in writing, and we'll walk you through every page.

Accountable at the top. Fairoaks IT is owned and run by Tom and Adam Crossley. If something isn't right, the people who own the company are the people who answer for it.

From our Client Bill of Rights:

- Answers to your questions in plain English
- All costs explained up front, with no hidden fees
- A single point of contact for every technology issue, including help with your other vendors
- Your request acknowledged within an hour

Who we are

About Fairoaks IT

An independent, owner-led managed IT and cybersecurity company. Tom Crossley founded Fairoaks IT in 1991, and he and his son, Adam Crossley, own and run it today.

We support CPA, accounting, bookkeeping and tax firms across Eastern Massachusetts, Rhode Island and the Charlotte, NC area from offices in Franklin, MA and Belmont, NC.

Soteria Award winner
Most Trusted MSP in North America

Microsoft Partner. Certified Trust Level 2 IT provider. As seen on MarketWatch, Newsmax, Business Insider and FOX 28.

<12 min Average time to start on a support issue	**99.98%** Average network uptime for fully managed clients	**98%** End-user satisfaction

What our clients say

"Our server and network infrastructure is demanding. We have hundreds of clients that use RDS on our servers, and Fairoaks IT makes sure it just plain works."

Mark Kilduff
Owner, Remote Quality Bookkeeping

"I have been working with Fairoaks IT for decades. They have always been so quick to resolve any issues I've had. I totally trust Fairoaks IT and I like the fact that they keep me informed of the latest cybersecurity threats."

AL

Ann Lorenz
Owner, Ann Lorenz Bookkeeping

"I can sleep at night knowing that Fairoaks IT is diligent in ensuring the safety of my systems... whenever I call, someone always answers the phone live."



Larry Zaharoff
Attorney, Zaharoff Law

"Tom and Adam are always accessible too, so when we do need to review our account and service, you are available to us."



Kevin Lagasse
Executive Vice President, The Lagasse Group

Ready for straight answers about your IT?

Schedule a discovery call: a straightforward conversation about your firm, your tax software and what isn't working. No pitch and no pressure. If we're not the right fit, we'll tell you.

fairoaksit.com/discoverycall

Franklin, MA

1000 Franklin Village Dr, Suite 303
Franklin, MA 02038
(774) 222-5500

Eastern Massachusetts and Rhode Island

Belmont, NC

32 North Main Street, Suite 206
Belmont, NC 28012
(704) 440-9016

The Charlotte, NC area

fairoaksit.com/industries/accounting

Fairoaks IT
Cybersecurity | AI Advisory | Managed IT | Cloud

Soteria Award winner: Most Trusted MSP in North America

© 2026 Fairoaks IT. General information, not legal advice.