Fairoaks IT
Cybersecurity | AI Advisory | Managed IT | Cloud

2026 edition

# Before You Hire (or Fire) Your IT Company

## The Professional Firm's Q&A Guide

Straight answers for partners, owners and office managers at law firms, engineering and architecture firms and other professional practices, plus five tools you can put to work this week.

Soteria Award winner
**Most Trusted MSP in North America**

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

## What's inside


| | |
|---|---|
| The 2-minute scorecard | 3 |
| Is it time to fire your IT company? | 4 |
| Files, software and remote work | 5 |
| Confidentiality and client trust | 7 |
| Security and fraud | 10 |
| Cost, contracts and switching | 12 |
| 10 questions to ask before you sign | 15 |
| Tool 1: Client data handling policy | 16 |
| Tool 2: Wire and payment verification policy | 17 |
| Tool 3: Employee offboarding checklist | 18 |
| Tool 4: AI use policy starter | 19 |
| Tool 5: Questionnaire and insurance prep sheet | 20 |
| What happens in an assessment | 21 |
| About Fairoaks IT | 22 |


### From the desk of Tom Crossley

Law firms, engineering firms and other professional practices have been part of Fairoaks IT for more than 30 years. Over that time, the technology has changed completely. The expectation hasn't: your clients trust you with their information, and they expect you to protect it.

Today that trust gets tested in new ways. A client sends a security questionnaire before the next engagement. A closing email changes the wire instructions. A model that took a minute to open now takes ten, and a partner is working from a hotel on a phone.

When your technology works, nobody notices. When it doesn't, the cost shows up as unbilled time, missed deadlines and uncomfortable conversations with clients.

The most common story I hear from firms isn't about a hacker. It's about a partner who is paying an IT company and still managing every problem personally.

So we 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 files, confidentiality, fraud and cost
- 10 questions to ask any IT company before you sign
- five tools you can copy and use this week

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



**Tom Crossley**
Founder and President, Fairoaks IT

Start here

# The 2-minute scorecard: is your IT built for a professional firm?

Check yes only if you're sure. "I think so" counts as no. That isn't us being tough; it's how a client's security team or your insurance carrier will see it.

| | | | |
|---|---|---|---|
| 1 | When someone calls for IT help, a real person starts on it within minutes, not hours. | ☐ Yes | ☐ No |
| 2 | Every login to email, document management and remote access uses multi-factor authentication. | ☐ Yes | ☐ No |
| 3 | Client files are organized so each matter or project is limited to the people working on it. | ☐ Yes | ☐ No |
| 4 | Clients send and receive documents through a secure portal or encrypted email, not plain attachments. | ☐ Yes | ☐ No |
| 5 | There's a written rule: any change to payment or wire instructions is verified by phone, using a number already on file. | ☐ Yes | ☐ No |
| 6 | Files and billing data are backed up where ransomware can't reach them, and were test-restored in the last 90 days. | ☐ Yes | ☐ No |
| 7 | Laptops are encrypted, and a lost phone with firm email can be wiped. | ☐ Yes | ☐ No |
| 8 | Big design files open quickly in the office and for remote staff. | ☐ Yes | ☐ No |
| 9 | Departing employees lose access to every system the day they leave. | ☐ Yes | ☐ No |
| 10 | You could answer a client's security questionnaire this week, with proof. | ☐ Yes | ☐ No |
| 11 | Your firm has a written policy on which AI tools can be used with client information. | ☐ 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 this quarter, starting with MFA, payment verification and backups.

### 5 to 7 yes

You're carrying more risk than you probably realize. One bad email could cost a client or a closing.

### 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 organizations 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 software.

If you’ve had to explain what Clio, NetDocuments, Revit or Deltek 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 go quiet on client questionnaires.

A client asks how you protect their data, and suddenly nobody has an answer.

## 6

### Remote work is a daily struggle.

Slow VPNs, files that won’t sync and partners emailing documents to themselves.

## 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 disrupting deadlines during a switch?** That fear keeps a lot of firms stuck with IT support they don’t like. Page 14 walks through what a clean switch looks like, step by step.

Chapter 1

# Files, software and remote work

Your work lives in documents and models. This chapter covers organizing them, keeping them fast and reaching them securely from anywhere.

## Document management system, or regular file folders?

For most firms beyond a few people, a document management system pays for itself. Tools like NetDocuments, iManage and Worldox organize files by client and matter, track versions, control who can see what and make everything searchable. Regular file shares can work for small firms, but they need careful permissions and folder structure to keep matters separate. Moving existing files takes planning, so nothing gets lost along the way.

## How do we make big CAD and Revit files work?

Match the setup to how your team collaborates:

- Workstations with dedicated graphics, plenty of memory and fast storage
- A fast office network, because large models punish slow switches and Wi-Fi
- Cloud collaboration tools like Autodesk Construction Cloud or Egnyte that sync files locally
- Remote access that doesn't push huge files over a slow VPN

Look at your file sizes, offices and workflows first, then pick the combination that actually performs.

Chapter 1, continued

## Files, software and remote work

**Quick win**

Schedule software updates around month-end billing and big deadlines, never during them.

### Should we move our files to the cloud?

Often, but not always all at once. Cloud document management and file sharing make remote work easier and take aging servers off your plate. Very large design files, older applications and slow internet connections can make a hybrid approach the better fit. Weigh your software, file sizes, internet reliability, client requirements and what your current server would cost to replace.

### How can attorneys and engineers work securely from anywhere?

With company-managed devices, multi-factor authentication on every login and secure access to your document system and applications, so client files never live on personal computers or personal cloud accounts. Phones and tablets that receive firm email should be managed, so a lost device can be wiped.

### How do we protect billing and accounting systems?

Treat them as business-critical. Time and billing software like Tabs3, PCLaw, Clio, Deltek and BQE Core, along with QuickBooks and Sage, should be backed up, kept current and protected with multi-factor authentication, with access limited to the people who need it.

Chapter 2

# Confidentiality and client trust

Clients trust you with their information. This chapter covers what that trust requires, from ethics rules to client questionnaires.

## What do lawyers' ethics rules say about technology?

The ABA Model Rules expect lawyers to understand the benefits and risks of the technology they use and to make reasonable efforts to prevent unauthorized access to client information. Several ABA formal opinions go further:

- **Formal Opinion 477R:** securing communications of client information
- **Formal Opinion 483:** what lawyers should do after a data breach
- **Formal Opinion 512:** using generative AI tools

Your state's version of the rules controls, so check with your bar, but reasonable security is the expectation everywhere.

## Do engineering, architecture and consulting firms have similar duties?

Usually by contract rather than ethics rules. Client agreements and NDAs increasingly spell out how drawings, data and communications must be protected, and firms working on defense projects may handle controlled unclassified information, which brings NIST SP 800-171 and CMMC requirements. Read your contracts for security clauses and ask clients what they expect.

## Confidentiality and client trust

**$3 billion**

Business email compromise losses reported to the FBI in 2025, most of it sent by wire transfer or ACH.

### How do we answer a client's security questionnaire?

Honestly, with proof. More clients, especially corporate, financial and healthcare clients, now ask outside firms about multi-factor authentication, encryption, backups, training and incident response before they send work. Gather evidence for every yes, keep a master copy of your answers so the next one takes an hour instead of a week, and where the honest answer is no, show a plan with dates. Tool 5 on **page 20** helps.

### What should a firm do after a data breach?

Follow your written plan. Monitor for breaches, act quickly to stop them and restore systems, determine what happened, and notify affected clients when their information was involved. State breach laws can require notice to individuals and regulators too. Call your IT provider and your cyber insurance carrier right away, and preserve evidence.

Chapter 2, continued

## Confidentiality and client trust

**Worth knowing**

Massachusetts firms holding residents' personal information also need a written information security program under 201 CMR 17.00.

### Can our firm use AI tools with client information?

Yes, carefully. ABA Formal Opinion 512 says lawyers using generative AI must protect client confidentiality, understand the tools' risks, review the output and, in some cases, get client consent. Free and personal AI accounts may keep what you type in, so client information only goes into business-grade tools approved for it. Start with the policy on **page 19**.

### How should client files be shared?

Through a secure client portal or encrypted email, not plain attachments. Portals track who downloaded what, set expiration dates and keep sensitive files out of inboxes. Write down the rules, including what never goes by regular email, with the policy on **page 16**.

### Who should be able to see each matter or project?

Only the people working on it. Access by client and matter, or by project, limits the damage if one account is compromised, and makes conflicts and ethical walls easier to enforce.

Chapter 3

# Security and fraud

Firms are targeted for the information they hold and the money they move. This chapter covers the threats and the basics that stop most of them.

## Why are professional firms targeted?

Because firms hold valuable, confidential information and move money. Law firms handle settlement and closing funds and hold client secrets, and design firms hold drawings clients expect them to protect. Criminals also know firms can't afford downtime or a public breach.

## How do we stop wire fraud on closings and settlements?

Verify every change to payment instructions by phone, using a number you already have on file, never one in the email. Business email compromise often arrives from a real, hacked mailbox at a title company, client or opposing counsel, so the email itself looks legitimate. Watch for:

- New or changed bank details, especially close to a closing or settlement
- Urgency and pressure to skip the usual steps
- Email addresses that are one character off

Put the rule in writing with the policy on **page 17**.

Chapter 3, continued

## Security and fraud

**Software we support**

Clio, MyCase, PracticePanther, Smokeball, PCLaw, Tabs3, NetDocuments, iManage, Worldox, AutoCAD, Revit, Civil 3D, Bluebeam, SolidWorks, Adobe, Deltek, BQE Core, Egnyte, Autodesk Construction Cloud, QuickBooks, Sage and Microsoft 365.

### What security basics should every firm have?

- Multi-factor authentication on email, document management and remote access
- Encryption on laptops and in transit
- Endpoint protection on every computer and server
- Email filtering for phishing and lookalike domains
- Security updates on a schedule someone checks
- Backups that ransomware can't reach, test-restored
- Staff training with phishing simulations

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 should happen when someone leaves the firm?

Remove access the same day from every system, collect devices, remove firm data from personal phones and move their files and matters to the right people. Use the checklist on **page 18**.

Chapter 4

# Cost, contracts and switching

This is where most IT relationships go right or wrong: how IT companies charge, what to watch for in a contract and how to switch cleanly.

## 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 month, and the provider makes more money when your systems have more problems.
- **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.

Some form of managed services almost always makes the most sense. Our IT Buyer's Guide covers each model, and typical industry pricing, in detail.

## 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 subscriptions are almost always extra, and bigger projects are usually quoted separately.

Ask specifically about onsite time, after-hours help, adding and removing users, and new hardware setup. At Fairoaks IT, 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, step by step.

## How do we switch IT providers without disrupting deadlines?

With a plan built around your schedule. A clean switch looks like this:

1. Discovery before anything changes: every system, password, license and vendor documented
2. A coordinated handoff from your current provider. Nobody flips a switch on a Friday afternoon.
3. Changes scheduled around court dates, submittals and month-end billing
4. The biggest risks fixed first, like backups and multi-factor authentication
5. One named point of contact and weekly check-ins until onboarding is done

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

## Should we just hire an IT person instead?

For most firms, one internal hire is the riskier choice. One person can't be an expert in networks, security, document management and CAD performance at once, and they take vacations and sick days. When they leave, what they know leaves with them.

If you already have a good IT person, 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?

**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 practice and design software do you support today?

**A good answer:** Names you recognize, like Clio, NetDocuments, Revit or Deltek, without you explaining them.

### 4 How will you protect client confidentiality?

**A good answer:** Specifics: multi-factor authentication, encryption, access by matter or project and secure file sharing.

### 5 Can you help us answer client security questionnaires?

**A good answer:** Yes, with proof behind every answer and a plan for any gaps.

### 6 How do you make big design files work for remote staff?

**A good answer:** A recommendation based on your file sizes and workflows, not a one-size-fits-all VPN.

### 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 deadlines?

**A good answer:** A documented plan scheduled around your calendar, 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 a firm you support?

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

> **How we answer them:** our average time to start on an issue is under 12 minutes, the software list is on **page 11**, we help firms answer client questionnaires, and our agreement spells out what's included before you sign.

Tool 1

# Client data handling policy starter

Copy and use

Fill in the blanks, share it with everyone in the firm, and review it once a year.

## _____ Client Data Handling Policy

1. Client files are stored only in _____, our approved document system, never on personal devices or personal cloud accounts.
2. Access to each client matter or project is limited to the people working on it.
3. We share files with clients through _____ or encrypted email, never as plain attachments for sensitive documents.
4. We never send Social Security numbers, bank account numbers or confidential documents by regular email.
5. Every login to firm systems uses multi-factor authentication.
6. Lost or stolen devices are reported to _____ immediately, so they can be locked and wiped.
7. Client files are retained for _____ years, then destroyed securely.

_____ _____

Approved by Date

Tool 2

# Wire and payment verification policy

Copy and use

This one policy stops most wire fraud. Have everyone who touches payments, closings or settlements sign it.

## _____ Payment Verification Policy

1. We never change wire or payment instructions based on an email, text, voicemail or letter alone.
2. Every change is verified by phone, using a number we already have on file or from the signed agreement. We never use contact details from the request itself.
3. Before any closing or settlement disbursement, _____ confirms the wire instructions by phone with the recipient.
4. A second person approves any wire over $_____.
5. We tell clients, in writing, that we will never change our wire instructions by email.
6. Urgency, secrecy or pressure is a reason to slow down, not speed up.
7. If we suspect fraud, we stop the payment and call our bank immediately, then report it at ic3.gov.

Approved by _____ Date _____

**Tell your clients too:** "We will never send you new wire instructions by email. Before sending money, call us at a number you already know."

Tool 3

# Employee offboarding checklist

Print and use

Use it for every departure, including attorneys, engineers, staff and contractors. Finish it the same day they leave.

| Name | Role | Last day | Completed by |
|---|---|---|---|
| | | | |

## Before and on the last day

- [ ] Disable accounts and sign them out of every session
- [ ] Remove access to email, document management, practice software and remote access
- [ ] Remove any banking, trust account or payment approval authority
- [ ] Remove firm email and data from personal phones
- [ ] Collect laptops, keys, badges and tokens

## Within a week

- [ ] Move their files, matters and projects to the right people
- [ ] Coordinate any client file transfers properly, rather than letting folders be copied
- [ ] Change shared passwords they knew
- [ ] Tell key clients and vendors who their new contact is
- [ ] Wipe returned devices before reissuing them

Tool 4

# AI use policy starter

Copy and use

Five rules cover most of the risk. Revisit them every few months as the tools change.

## _____ AI Use Policy

1. **Approved tools:** _____. Use them only with firm accounts, never personal ones.
2. **Never enter** client confidential information, privileged material, drawings or data covered by an NDA into a tool that isn't approved for it.
3. **Always review** AI output before it goes to a client, a court or a job site. AI tools make confident mistakes.
4. **Ask first.** Check with _____ before trying a new AI tool, browser extension or plug-in.
5. **When in doubt, leave it out,** and consider whether the client should be told or asked.

_____ _____

Approved by Date

Tool 5

# Client questionnaire and cyber insurance prep sheet

Print and use

Clients and carriers ask about the same controls. Gather the proof once and keep it current.

| Control | What they usually ask | Proof to have ready | In place? |
|---|---|---|---|
| **Multi-factor authentication** | Is MFA required for email, remote access and admin accounts? | A report showing MFA status for every user | ☐ Yes ☐ No |
| **Endpoint protection** | Is endpoint detection and response on every computer and server? | A device list from the security console | ☐ Yes ☐ No |
| **Encryption** | Are laptops and file transfers encrypted? | Encryption status report | ☐ Yes ☐ No |
| **Backups** | Are backups offline or unchangeable? When were they last tested? | A backup report and the date of the last test restore | ☐ Yes ☐ No |
| **Patching** | How quickly are critical updates applied? | A patch compliance report | ☐ Yes ☐ No |
| **Security training** | Do employees get training and phishing tests? | Training completion records | ☐ Yes ☐ No |
| **Access control** | Is access to client files limited to the people who need it? | Your access model by matter or project | ☐ Yes ☐ No |
| **Payment verification** | Do you verify payment changes by phone? | Your signed verification policy (Tool 2) | ☐ Yes ☐ No |
| **Incident response** | Do you have a written plan for a cyber incident? | The plan, with names and phone numbers | ☐ Yes ☐ No |

**Before you send it:** go through it line by line with your IT provider, ask for the proof rather than a "yep, we've got that," fix any gaps before the deadline, and confirm with your insurance agent what your policy requires.

Next step

# What happens in a Fairoaks IT assessment

We look at your technology the way you'd review a client's file: 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

- Network, firewall and Wi-Fi
- Servers, cloud storage and document management
- Practice, billing and design software
- Microsoft 365 and email security
- Backups, and whether they can actually be restored
- Security tools and updates
- Remote access and mobile devices
- Client and 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 law firms, engineering and architecture firms, surveyors and consultants 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**<br>Average time to start on a support issue | **99.98%**<br>Average network uptime for fully managed clients | **98%**<br>End-user satisfaction |

## What our clients say

"Fairoaks IT has the knowledge to fix our problems, we can't function as a business if the computers aren't working, and you make sure we are never down for long... If you're on the fence about switching IT companies, this isn't a hard decision, just do it."



**Steven Greenwald**
Attorney, Greenwald & Greenwald

"It's also great knowing that I can pick up the phone or email with the owners of the business if I have an issue. Fairoaks IT is the real deal."



**Ross Trethewey**
Owner, TE2 Engineering

"Fairoaks IT has let us focus on our business. When an IT issue pops up, they're right there to resolve it, quickly, and efficiently."



**Dennis O'Brien**
Owner, Dennis O'Brien Land Surveying

"Since joining Fairoaks as a client, I can focus on what I do best, and leave all things IT to them. That sense of security and trust is priceless to me."

SC

**Susan Rossi Cook**
Attorney and Mediator

# Ready for straight answers about your IT?

Schedule a discovery call: a straightforward conversation about your firm 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/professional-services


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.