Fairoaks IT

Cybersecurity | AI Advisory | Managed IT | Cloud

2026 edition

Before You Hire (or Fire) Your IT Company

The Construction Owner's Q&A Guide

Straight answers for owners, CFOs and operations leaders of construction companies, plus five tools you can put to work this week.

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
Job sites, trailers and field teams	5
Security, fraud and insurance	7
Software, hardware and files	10
Cost, contracts and switching	12
10 questions to ask before you sign	15
Tool 1: Payment-change verification policy	16
Tool 2: Employee offboarding checklist	17
Tool 3: AI use policy starter	18
Tool 4: Job site mobilization IT checklist	19
Tool 5: Cyber insurance prep sheet	20
What happens in an assessment	21
About Fairoaks IT	22

From the desk of Tom Crossley

If you run a construction company, you didn't get into the business to manage computers. You got into it to build. But somewhere along the way, technology became part of every job: plan sets in the trailer, Procore on the super's phone, payroll in Sage, bids flying back and forth by email.

When that technology works, nobody notices. When it doesn't, it shows up as a crew waiting on a drawing, a missed deadline, or a wire transfer that went to the wrong account.

Construction companies have been a big part of our client base since I started Fairoaks IT in 1991. The most common story I hear isn't about a hacker. It's about an owner who is paying an IT company and still managing every problem personally.

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 to the questions contractors ask us most
- 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, I'll tell you.



Tom Crossley
Founder and President, Fairoaks IT

Start here

The 2-minute scorecard: is your IT built for construction?

Check yes only if you're sure. "I think so" counts as no. That isn't us being tough; it's how 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.	☐ Yes	☐ No
2	Every job site trailer is set up the same way, with a backup internet connection.	☐ Yes	☐ No
3	Company phones and tablets are managed, so a lost device can be locked and wiped remotely.	☐ Yes	☐ No
4	Every email account, including the owner's, uses multi-factor authentication.	☐ Yes	☐ No
5	There's a written rule: any change to payment instructions is verified by phone, using a number already on file.	☐ Yes	☐ No
6	Backups are stored where ransomware can't reach them, and someone has test-restored them in the last 90 days.	☐ Yes	☐ No
7	Your Microsoft 365 email and files have their own backup, separate from Microsoft.	☐ Yes	☐ No
8	When someone leaves, their access is shut off the same day, using a checklist.	☐ Yes	☐ No
9	You could show proof for every "yes" on your cyber insurance application.	☐ Yes	☐ No
10	Estimators and PMs have computers sized for Bluebeam, AutoCAD and takeoff software.	☐ Yes	☐ No
11	Admin passwords and network details are documented, and more than one person can get to them.	☐ 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 backups, MFA and payments.

5 to 7 yes

You're carrying more risk than you probably realize. One bad email or failed drive could stop work.

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 contractors 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 Procore, Sage or Bluebeam is, they’re learning on your dime.

4

Nobody can tell you if your backups work.

Ask when they last did a test restore. A vague answer is the answer.

5

Field calls go nowhere.

Your supers have stopped calling for help. They call the office instead, and the office calls you.

6

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.

7

The invoices surprise you.

Extra charges for things you thought were covered, and projects that cost more than the quote.

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 the disruption of switching?** That fear keeps a lot of contractors stuck with IT support they don’t like. Page 14 walks through what a clean switch looks like, step by step.

Chapter 1

Job sites, trailers and field teams

Your company doesn't work in one building. It works in a dozen temporary ones, many with weak signal and borrowed power. This chapter covers getting sites connected, keeping field teams working and closing sites out cleanly.

What does a good job site trailer setup actually include?

More than a hotspot taped to the wall. A setup that holds up for the life of a project has:

- Business-grade networking equipment with a firewall, not a consumer router
- A primary internet connection plus a backup from a different source, so one carrier outage doesn't stop the day
- Separate Wi-Fi networks for your team and for guests, subs and cameras
- Battery backup and surge protection, because temporary power is rough on electronics
- Remote monitoring, so your IT provider knows the trailer is down before your super calls

Most important, every trailer should be set up the same way. When every site is identical, every site is supportable. At Fairoaks IT, our proprietary trailer setup arrives configured and ready, which is how we get new sites online within days.

How far ahead should we plan IT for a new job site?

As soon as the job is on the schedule. The longest lead time is almost always the internet carrier, and you can't speed that up once you're waiting. Order service as soon as you have a site address, decide what the backup connection will be, and work out who needs which devices before mobilization day.

Set up project folders and sharing permissions for subs, the architect and the owner ahead of time, too, so nobody is emailing drawings around in week one. The job site mobilization checklist on **page 19** walks through it step by step.

What should happen when a superintendent needs IT help from the field?

They should reach a real person who knows your setup, fast. Ask any IT provider three things: how quickly a person actually starts on an issue, what happens after hours, and whether your field people can reach them directly instead of going through the office.

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. Most field problems can be fixed remotely in minutes. When they can't, we get someone onsite.

Chapter 1, continued

Job sites, trailers and field teams

Quick win

Post the IT support number in every trailer. Not the Wi-Fi password.

Don't skip this

Archive project files and close sharing links before the trailer leaves the site.

Why do plan sets take forever to open in the field, and what fixes it?

Usually it's one of three things. The file is coming from the office server over a VPN connection that was never built for 400 MB drawings. The trailer's internet is too slow or shared by too many people. Or the laptop doesn't have the memory and graphics power the software needs. The fixes:

- Keep active drawings in a tool built for large files, like Bluebeam Studio, Procore, Autodesk Construction Cloud or a properly configured SharePoint setup
- Sync only the projects each site actually needs
- Size the trailer connection for real plan sets, not email
- Match laptops to the work people do

You rarely need all four. A good IT provider will tell you which one is your bottleneck.

How should we handle phones and tablets for crews who come and go?

With mobile device management, usually called MDM. It lets your IT provider set up every company phone and tablet the same way, push the apps your crews need, require a passcode, keep company data separate from personal data, and lock or wipe a device that disappears off a site.

For personal phones that get company email, MDM can remove just the company data when someone leaves, without touching their photos. At Fairoaks IT, phone and tablet management is available as an add-on to our managed IT plans.

What should happen to our IT when a job wraps up?

Demobilization deserves the same care as mobilization, and it almost never gets it. Before the trailer leaves:

- Archive the project files where you'll be able to find them years from now
- Close outside sharing links so subs and owners can't keep pulling documents
- Remove accounts for temporary staff and consultants
- Collect and wipe devices before they're reissued
- Cancel or transfer the internet service so you're not paying for a trailer that's gone

Closed jobs have a long tail. Warranty claims and disputes can surface years later, and your records are your best defense.

Chapter 2

Security, fraud and insurance

Most attacks on contractors don't start with hacking. They start with an email. This chapter covers the threats that actually hit construction companies and the basics that stop most of them.

Why do attackers go after construction companies?

Because construction makes it easy and profitable. Projects run on deadlines, so a contractor facing a missed milestone is more likely to pay. Work depends on shared files and lots of outside partners, which means lots of email and lots of chances to fool someone. And most construction firms don't have dedicated security staff.

It shows in the numbers: Rapid7 ranked construction among the three most-attacked sectors for ransomware in 2025. The good news is that attackers mostly go after easy targets. The basics on the next page make you a much harder one.

What does a fake payment request look like, and how do we stop it?

Usually it looks completely normal. An email from a sub or supplier you work with says they've changed banks and asks you to use new wiring instructions for the next payment. Often it really did come from their account, because their mailbox was hacked, not yours.

Watch for changed bank details, urgency ("we need this today"), requests to keep it quiet, and email addresses that are one character off.

The fix costs nothing: never change payment instructions without calling the vendor at a number you already have on file. Put it in writing with the policy template on **page 16**.

How should we protect bids and drawings we share with subs and owners?

Share from a system built for it, like Procore, Bluebeam Studio or SharePoint, instead of email attachments and personal file-sharing accounts. Give people the project folder they need, not your whole file server. Set links to expire and close them when the project closes. A link that never expires is a door that never closes.

$3 billion

Business email compromise losses reported to the FBI in 2025. 86% of that money moved by wire transfer or ACH.

What security basics should every contractor have?

If you do only these, you've closed most of the doors attackers use:

- Multi-factor authentication on every email account, including the owner's, and on remote access
- Endpoint protection on every computer and server
- Email filtering that catches phishing and lookalike domains
- Security updates applied promptly, on a schedule someone actually checks
- Backups stored where ransomware can't reach them, and test-restored regularly
- Security awareness training, so your team knows what a bad email looks like
- Separate admin accounts that aren't used for everyday email

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 with advanced threat detection.

What will our cyber insurance carrier ask, and why does it matter if we guess?

Carriers ask about the same core controls every year, and the questions get tougher: multi-factor authentication, endpoint detection and response, tested backups that can't be altered, security training, patching, and how you verify payment changes.

Here's the problem. The person filling out the application is often the office manager or controller, checking "yes" because they believe IT has it handled. If you file a claim and the controls you described weren't really in place, that's exactly what the carrier will look at. Walk through the questionnaire with your IT provider line by line and ask for proof. The prep sheet on **page 20** makes it easy. Your insurance agent has the final word on your policy.

Worth knowing

Data rules follow where your employees live. A Massachusetts contractor with Rhode Island employees has two sets of rules.

Do state data security rules apply to us?

Probably, because you hold employee Social Security numbers, driver's license numbers and bank details for payroll. A few to know:

- **Massachusetts:** 201 CMR 17.00 requires a written information security program (WISP) and specific safeguards, including encryption on laptops and over public networks.
- **Rhode Island:** requires a risk-based information security program, and notice to affected residents within 45 calendar days of confirming a breach.
- **North Carolina:** requires notifying affected residents without unreasonable delay, and notifying the Attorney General's Consumer Protection Division.
- **South Carolina** has its own breach notification law, too.

Rules follow where your people live, not just where your office is. This is general information, not legal advice; your attorney has the final word.

Can our team safely use AI tools with bids and project documents?

Yes, with the right tools and a few rules. AI is useful for the paperwork side of construction: drafting RFIs and transmittals, summarizing specs, cleaning up meeting notes. The risk is in how it's happening. Personal accounts and free tools may keep what your team types in, and nobody knows who's using what.

Banning AI rarely works; people just use it on their phones. An approved option with clear rules does. If you're on Microsoft 365, you may already have a business-grade option. Start with the AI use policy on **page 18**.

Chapter 3

Software, hardware and files

The software that runs your company is specialized and demanding. This chapter covers who owns problems, what hardware your people need and where your data should live.

Who should own a problem between our software vendor and our network?

Your IT provider, every time. Software vendors support their application. They don't support your server, your network, your Wi-Fi or the laptop it runs on, so problems in between bounce back and forth while your team waits. "It's a network issue." "It's a software issue." Meanwhile the estimate is due Friday.

The right setup is one point of contact that takes ownership: opens the case with the vendor, provides the logs and details the vendor asks for, and stays on it until it's fixed. At Fairoaks IT, vendor coordination is part of our fully managed service, and our Client Bill of Rights promises a single point of contact for every technology issue, including help with your other vendors.

What computers do estimators, project managers and supers need?

Different ones. Buying one standard machine for everybody wastes money in one direction or the other.

- **Estimators and anyone in CAD:** a current-generation processor, generous memory, a dedicated graphics card, fast solid-state storage and two large monitors
- **Project managers:** a capable laptop that handles Bluebeam and large PDFs, plus a dock and monitors for office days
- **Superintendents:** a durable laptop or tablet that survives the truck and the trailer, with a protective case and a spare charger
- **Office staff:** standard business machines are fine

Then plan replacements on a schedule instead of waiting for failures. A slow computer costs an estimator time every day. A failed one the week of a bid costs a lot more.

Chapter 3, continued

Software, hardware and files

Software we support

Procore, Sage 300 CRE (Timberline), Sage 100 Contractor, Bluebeam, AutoCAD, Autodesk Construction Cloud, PlanGrid, On-Screen Takeoff, Trimble, Foundation, ProContractor, ConEst (IntelliBid), Bid2Win, Chief Architect, Xactimate, Master Builder and Microsoft 365.

Should Sage and our files live on a server or in the cloud?

It depends, and anyone who gives you a one-word answer without looking at your setup is guessing. Cloud hosting makes remote access easier, gets aging hardware out of your office and can simplify backup. A well-maintained local server can still be faster for very large files, and some accounting and estimating software versions run best on premises.

The questions that decide it: which versions of Sage and your other applications you're on, how many people work from the field, how good your office and trailer connections are, and what it would cost to replace your current server. We lay out both options side by side, with costs, before anything moves.

Are we getting what we pay for from Microsoft 365?

Often not. Many contractors pay for Microsoft 365 licenses that include security and file-sharing features they've never turned on. A quick review usually finds the same four things:

- Multi-factor authentication not enforced for everyone
- SharePoint and OneDrive set up without a plan, so files end up everywhere
- Outside sharing left wide open
- No separate backup

That last one surprises people. Microsoft keeps 365 running, but that isn't the same as promising to get back every file someone deleted, overwrote or had encrypted months ago. Fixing these four things is one of the highest-value IT projects a contractor can take on.

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 disrupting your jobs.

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. Worse, the provider makes more money when your systems have more problems, so nobody is paid to prevent them. All the risk sits with you.
- **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, which lines up their interests with yours.
- **Software vendor support:** help with one application only. Useful, but it stops at the edge of their software.

For a contractor with real infrastructure and job sites, some form of 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 subscriptions are almost always extra, and bigger projects like a server replacement or a new office buildout are usually quoted separately.

Ask specifically about onsite time, after-hours help, adding and removing users, and new hardware setup. At Fairoaks IT, our plans cover labor, hardware and software are billed separately, and we explain every cost up front.

Chapter 4, continued

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 active projects?

With a plan. A clean switch looks like this:

1. Discovery before anything changes: every system, password, license and vendor documented, at the office and the job sites
2. A coordinated handoff from your current provider. Nobody flips a switch on a Friday afternoon.
3. A schedule built around your bid dates, payroll and month-end billing
4. The biggest risks fixed first, like backups and multi-factor authentication, with bigger projects saved until things are stable
5. One named point of contact and weekly check-ins until onboarding is done
6. Your team knowing exactly how to get help on day one

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 contractors, one internal hire is the riskier choice. One person can't be an expert in networks, security, cloud, Microsoft 365 and construction software at once, can't be in two places when the office and a trailer both go down, and takes 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 for security, coverage, vacations and big projects, 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? Can you show me the numbers?

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

2 What happens when something breaks after hours?

A good answer: A clear process for emergencies: what's covered and exactly how to reach them.

3 Have you set up job site trailers? What's in your setup?

A good answer: Specific equipment, a backup connection, remote monitoring and a timeline in days, not weeks.

4 Which construction applications do you support today?

A good answer: Names you recognize, like Procore, Sage and Bluebeam, without you having to explain them.

5 Who owns a problem between you and our software vendor?

A good answer: "We do." They open the case and stay on it until it's fixed.

6 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."

7 What isn't included in the monthly fee?

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

8 What does onboarding look like, step by step?

A good answer: A documented plan with a point of contact, a timeline 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 construction client?

A good answer: A clear, written answer, and references from companies 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, our proprietary trailer setup, the software list on **page 11**, and an agreement that spells out what's included before you sign.

Tool 1

Payment-change verification policy

Copy and use

This one policy stops most payment fraud. Copy it onto your letterhead, fill in the blanks, and have everyone who touches payments sign it.

_____ Payment Change Verification Policy

Effective date: _____

1. We never change payment instructions (bank name, account or routing numbers, payment method or remittance address) based on an email, text, voicemail or letter alone.
2. Every change request is verified by phone, using a number we already have on file or from the signed contract. We never use a phone number, link or contact listed in the request itself.
3. A second person, _____, approves every change to payment instructions before it takes effect.
4. Any payment over $_____ requires a second approver, even when the instructions haven't changed.
5. We document each verification: who called, who they spoke to, the number used, and the date and time.
6. Urgency, secrecy or pressure ("we need this today," "please keep this between us") is a reason to slow down, not speed up.
7. If we suspect fraud, we stop the payment and notify _____ and our IT provider immediately. If money has already been sent, we call our bank right away and file a report at ic3.gov.

Name and role	Signature	Date
Name and role	Signature	Date

Why the call matters: when a sub's mailbox has been hacked, the fraudulent email comes from their real address. The only reliable check is a phone call to a number you already trust.

Tool 2

Employee offboarding checklist

Print and use

Use it for every departure, including subcontractors and temporary staff who had system access. Finish it the same day they leave.

Name	Role	Last day	Completed by

Before the last day

- [ ] List every system they use: email, Microsoft 365, Procore, Bluebeam, Sage, supplier and bank portals, plan rooms
- [ ] List shared passwords they know: shared mailboxes, job site Wi-Fi, alarm and gate codes
- [ ] Move ownership of their files, project folders and shared links to their manager
- [ ] List every company device they have

On the last day

- [ ] Disable their accounts and sign them out of every session
- [ ] Remove their multi-factor authentication devices
- [ ] Remove company email and data from personal phones
- [ ] Remove them from project apps, portals, plan rooms and distribution lists
- [ ] Remove any banking or payment approval authority
- [ ] Change shared passwords, job site Wi-Fi passwords, and alarm and gate codes they knew
- [ ] Collect the laptop, tablet, phone, chargers, keys, fobs and badges
- [ ] Give their manager access to their email and files

Within a week

- [ ] Tell key vendors and subs who their new contact is
- [ ] Wipe returned devices before reissuing or retiring them
- [ ] File this checklist with the employee record

Tool 3

AI use policy starter

Copy and use

Five rules cover most of the risk. Fill in the blanks, share it with everyone, and revisit it every few months as the tools change.

_____ AI Use Policy

1. **Approved tools:** _____. Use them only with company accounts, never personal ones.
2. **Never enter** bid pricing or estimates, contracts, client or owner financial information, employee personal information, passwords, or anything covered by an NDA.
3. **Always review** AI output before it goes to a client, owner, architect or sub. 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.**

Approved by _____ Date _____

Good places to start

- Drafting RFIs, transmittals and routine emails
- Summarizing long specs or meeting notes
- First drafts of job site memos and safety meeting outlines
- Turning field notes into punch lists

Ask before approving a tool

- Does it use our data to train its models?
- Can we manage accounts centrally and remove people when they leave?
- Does it work with our Microsoft 365 security settings?
- What happens to our data if we cancel?

Tool 4

Job site mobilization IT checklist

Print and use

Start this the day a job lands on the schedule. Internet installation is usually the longest lead time on the list.

Project	Site address	Mobilization date	Superintendent

As soon as the job is on the schedule

- [ ] Order primary internet service for the site address and confirm the install date
- [ ] Choose a backup connection from a different source
- [ ] Plan trailer power, battery backup and surge protection for IT equipment
- [ ] List who needs devices on site: super, PM, assistant, field engineers

Before mobilization

- [ ] Schedule the trailer setup (Fairoaks IT clients: request your proprietary trailer setup)
- [ ] Create the project folder structure and permissions
- [ ] Set up outside sharing for subs, the architect and the owner, with expiration dates
- [ ] Add the project and the right people in Procore, Bluebeam Studio or your project platform
- [ ] Plan for the printer or plotter, plus cameras or access control if needed

First week on site

- [ ] Test the connection by opening real plan sets, not just a speed test
- [ ] Confirm remote monitoring is reporting
- [ ] Post the IT support number in the trailer (not the Wi-Fi password)
- [ ] Confirm field devices are enrolled and working

At demobilization

- [ ] Archive project files where you'll find them years from now
- [ ] Close outside sharing links and remove temporary users
- [ ] Collect, wipe and reissue devices
- [ ] Cancel or transfer internet service and return the trailer equipment

Tool 5

Cyber insurance questionnaire prep sheet

Print and use

Questions vary by carrier, but these come up on almost every application. Gather the proof before renewal, not after a claim.

Control	What carriers 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 detection and response	Is EDR installed on every computer and server?	A device list from the security console	☐ 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? How often?	Training completion records	☐ Yes ☐ No
Email security	Is email filtered for phishing and malicious links?	A summary of email security settings	☐ Yes ☐ No
Payment verification	Do you verify payment changes by phone before sending money?	Your signed verification policy (Tool 1)	☐ Yes ☐ No
Incident response	Do you have a written plan for a cyber incident?	The plan, with names and phone numbers	☐ Yes ☐ No
Admin accounts	Are admin accounts separate and limited to the people who need them?	A list of admin accounts and who holds them	☐ Yes ☐ No

Before you sign the application: 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 renewal date, and confirm with your insurance agent what your policy and your contracts require.

Next step

What happens in a Fairoaks IT assessment

We look at your technology the way a good inspector looks at a building: 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 network, firewall and Wi-Fi
- Servers and computers, including whether they fit the software your people run
- Microsoft 365 and email security
- Backups, and whether they can actually be restored
- Security tools and updates
- Construction software and vendor setups
- Job site connectivity
- Cyber insurance and compliance 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 construction companies 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

"I used to do everything within the company regarding computers, email, web, etc. I was getting in over my head and needed to outsource our IT... Fairoaks IT is big enough to offer best in class service, yet small enough that you will be working with the same people all the time."



Kevin Ricciardelli
Owner, Excel Building Systems

"Fairoaks IT has the people that can solve our varied and multiple software issues quickly and efficiently."

Andy Leonard
Owner, WW Contracting Corp

"Fairoaks IT has always done everything they can to prevent us from any network downtime."



Mark Travis
President, Mass Installation

"If you are shopping for a new IT support partner, then focus on results and not on price. What is the cost of your business being down versus trying to save a few pennies on monthly or hourly fees?"



Rob English
Owner, Chemical Solutions

Ready for straight answers about your IT?

Schedule a discovery call: a straightforward conversation about your company, your job sites 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/construction-it

Fairoaks IT
Cybersecurity | AI Advisory | Managed IT | Cloud

Soteria Award winner: Most Trusted MSP in North America

© 2026 Fairoaks IT. State law summaries are general information, not legal advice.