Fairoaks IT
Cybersecurity | AI Advisory | Managed IT | Cloud

2026 edition

Before You Hire (or Fire) Your IT Company

The Manufacturer's Q&A Guide

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

Soteria Award winner
Most Trusted MSP in North America

Prepared by **Adam Crossley, CEO, 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
Plant floor, warehouse and uptime	5
Security, compliance and insurance	7
ERP, servers and software	10
Cost, contracts and switching	12
10 questions to ask before you sign	15
Tool 1: Payment-change verification policy	16
Tool 2: IT outage playbook	17
Tool 3: Employee offboarding checklist	18
Tool 4: AI use policy starter	19
Tool 5: Insurance and customer questionnaire prep	20
What happens in an assessment	21
About Fairoaks IT	22

From the desk of Adam Crossley

Before I worked in IT, I worked in manufacturing. At Sikorsky, on the Navy Seahawk program, I learned what every plant manager already knows: when one thing stops, everything behind it stops too.

Technology is now one of those things. The ERP schedules the work. The network connects the machines. The label printer decides whether the truck leaves on time. And more of your customers want proof that you protect their drawings and data.

When that technology works, nobody notices. When it doesn't, it shows up as a stopped line, a missed shipment or a customer questionnaire you can't answer.

The most common story I hear from manufacturers 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 manufacturers 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.



Adam Crossley
CEO, Fairoaks IT

Start here

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

Check yes only if you're sure. "I think so" counts as no. That isn't us being tough; it's how a customer audit or an 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	Production equipment, like CNC machines, is on its own network segment, separate from office computers.	☐ Yes	☐ No
3	Wi-Fi works everywhere scanners and tablets are used, including the back of the warehouse.	☐ 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 a supplier's payment instructions is verified by phone, using a number already on file.	☐ Yes	☐ No
6	ERP and file server backups are stored where ransomware can't reach them, and someone has test-restored them in the last 90 days.	☐ Yes	☐ No
7	You have a written plan for how production and shipping keep going if the ERP, server or internet goes down.	☐ Yes	☐ No
8	The server running your ERP, and its operating system, are still supported and getting security updates.	☐ Yes	☐ No
9	You know whether any contract requires NIST 800-171 or CMMC, and where that controlled data lives.	☐ Yes	☐ No
10	You could answer a customer's security questionnaire this week, with proof.	☐ 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 server could stop the line.

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 manufacturers 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 ERP.

If you’ve had to explain what Epicor, JobBOSS or NetSuite 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 ERP. A vague answer is the answer.

5

Second shift has given up calling.

When something breaks after 3:30, people wait until morning or call you at home.

6

They go quiet on customer requirements.

A security questionnaire or a NIST 800-171 clause shows 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 disrupting production during a switch?** That fear keeps a lot of manufacturers stuck with IT support they don’t like. Page 14 walks through what a clean switch looks like, step by step.

Chapter 1

Plant floor, warehouse and uptime

Your business doesn't stop at the office door. This chapter covers the machines, Wi-Fi, scanners and printers that keep product moving, and how to keep running when something fails.

How do CNC machines and other equipment get connected to the network safely?

Carefully, and on their own network. A good setup:

- Puts production equipment on its own network segment, separate from office computers and email
- Gets programs from engineering to the floor reliably, without someone walking a USB stick across the plant
- Controls how equipment vendors connect for remote support, so access is on when it's needed and off when it isn't
- Documents every connected machine: what it is, where it plugs in and who supports it
- Keeps older machine software away from the internet when it can't be updated

At Fairoaks IT, we help integrate equipment like CNC machines into your network and work alongside your equipment vendors when a machine needs their expertise.

How do we get Wi-Fi that actually works in a warehouse?

Design it for the building. Steel racking, high ceilings, machinery and long aisles block and bounce wireless signals, so access points need to go where scanners and tablets are actually used, not where it was easiest to run a cable.

Walk the building with someone who knows what to look for, or run a wireless survey in larger facilities, and fix the dead spots before buying more equipment. Business-grade access points managed from one place also make it easy to see which devices are struggling.

What should happen when someone on second shift needs IT help?

They should know exactly who to call and what to try first. 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. For multi-shift plants, we plan ahead: monitoring that catches problems overnight, a short guide for shift leads, and an agreed process for urgent issues outside business hours.

Plant floor, warehouse and uptime

Quick win

Keep one spare label printer and one spare scanner configured and ready on a shelf. It turns a two-hour outage into a two-minute swap.

Why do label printers and scanners keep failing?

Usually it's not the device. Scanners drop off when Wi-Fi is weak. Label printers fail when a driver updates, an address changes or the connection to the ERP or shipping software breaks. And nobody owns the problem, because it sits between your IT provider, your ERP vendor and your shipping software.

The fix is ownership: one team that keeps the network stable, documents how every printer and scanner is set up, keeps spares configured and ready, and calls the software vendor when the problem is on their side.

How do we keep shipping if the ERP, server or internet goes down?

With a plan written before you need it:

- Backups stored where ransomware can't reach them, and test-restored on a schedule
- A recovery target for each critical system, so everyone knows how long the ERP can be down
- A backup internet connection where an outage stops shipping
- Battery backup on servers and network closets, sized to shut down cleanly or reach a generator
- A floor-level playbook: who decides, how orders get picked and labeled by hand, and who calls customers

Tool 2 on **page 17** gives you an outage playbook to fill in.

How should we handle shared shop floor computers?

Lock them down, and give each person their own login when you can. Shared computers with one generic password make it impossible to know who did what, and they're a favorite way in for attackers. At a minimum, limit shared stations to the applications they need, keep them updated, block email and web browsing where they aren't needed, and remove anyone who leaves from every system the same day.

Chapter 2

Security, compliance and insurance

Manufacturers face more attacks than any other industry, and more customers now ask for proof of security before they buy. This chapter covers the threats, the requirements and the basics that handle most of both.

Why are manufacturers targeted more than other industries?

Because downtime is expensive and there are a lot of ways in. A stopped line costs money by the hour, so attackers expect manufacturers to pay. Plants also hold valuable designs and customer data, connect older equipment that can't always be updated, and trade a lot of email with suppliers and customers.

IBM's 2026 X-Force Threat Intelligence Index found manufacturing was the most targeted industry for the fifth year in a row. The good news: attackers mostly go after easy targets, and the basics on the next page make you a much harder one.

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

It usually looks completely normal. An email from a supplier you buy from says they've changed banks and asks you to use new instructions for the next invoice. Often it really did come from their account, because their mailbox was hacked, not yours. The FBI's 2025 Internet Crime Report recorded about $3 billion in business email compromise losses.

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 supplier at a number you already have on file. Put it in writing with the policy on **page 16**.

Security, compliance and insurance

27.7%

Share of the cyber incidents IBM X-Force observed in 2025 that hit manufacturing, the most of any industry for the fifth year in a row.

What security basics should every manufacturer have?

- Multi-factor authentication on every email account, including the owner's, and on remote access
- Endpoint protection on every computer and server
- Production equipment on its own network segment
- 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
- Controlled remote access for equipment and software vendors

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.

Does our company need CMMC right now?

Only if you work on Defense Department contracts or subcontracts, and the requirements are in flux. As of October 2026:

- Phase 1 self-assessments remain in effect for applicable contracts
- The Phase 2 requirement for third-party certification, originally set for November 10, 2026, was suspended in July 2026 pending a Defense Department review
- Contracts with DFARS 252.204-7012 still require you to protect controlled unclassified information under NIST SP 800-171
- Primes still flow requirements down to their suppliers

Watch for the outcome of the review, and don't treat the pause as a reason to stop preparing. We help manufacturers get ready, scoped as a project or compliance add-on.

Security, compliance and insurance

Worth knowing

CMMC rules are changing. Check the current status before you budget, and protect controlled data either way.

What is NIST 800-171, and how do we know if it applies?

NIST SP 800-171 is a set of 110 security requirements for protecting controlled unclassified information, or CUI, outside the federal government. It applies when a contract includes DFARS 252.204-7012 and you store, process or send CUI, such as certain drawings, specifications or technical data.

Start by reading your contracts and purchase orders for that clause, then find out where CUI actually lives: which systems, which folders, which people. The smaller you can make that footprint, the easier compliance gets.

How should we handle customer questionnaires and cyber insurance applications?

The same way: honestly, with proof. Customers and carriers ask about the same core controls, including multi-factor authentication, endpoint protection, tested backups, training, patching, incident response, and more and more often how production systems are separated from the office. Answer truthfully, gather proof for every yes, and keep a master copy so the next one takes an hour instead of a week. Tool 5 on **page 20** helps. Your insurance agent has the final word on your policy.

Can our team use AI tools with drawings and customer data?

Yes, with the right tools and rules. AI is useful for drafting work instructions, summarizing specs and writing quotes and emails. But personal accounts and free tools may keep what your team types in, and customer drawings, pricing and anything controlled under ITAR or defense contracts shouldn't go into tools that aren't approved for that data. Start with the AI use policy on **page 19**.

Chapter 3

ERP, servers and software

Your ERP runs the plant. This chapter covers who owns problems, where the ERP should live and what hardware your people need.

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

Your IT provider, every time. ERP vendors support their application. They don't support your server, your network or the computers on the floor, so problems in between bounce back and forth while orders wait. "It's a network issue." "It's a software issue." Meanwhile the trucks are at the dock.

The right setup is one point of contact that 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.

Should our ERP run in the cloud or on a server?

It depends, and anyone who gives you a one-word answer without looking at your setup is guessing. Hosted or cloud ERP simplifies remote access and takes aging hardware off your plate. An on-site server can still make sense when production has to keep running even if the internet goes down, or when your ERP version runs best locally.

The deciding factors: your ERP and version, your internet reliability, how many sites you run, and what it would cost to replace your current server. We lay out both options side by side, with costs, before anything moves.

ERP, servers and software

Software we support

Epicor, JobBOSS, Global Shop Solutions, NetSuite, SAP Business One, Microsoft Dynamics, Microsoft 365 and AutoCAD, plus EDI, barcode and label printing, and shipping systems.

Our ERP runs on an old server. What should we do?

Don't panic, but don't wait for it to fail either. Check three things this month:

1. Can your backups actually restore the ERP? Test it.
2. Is the server's operating system still getting security updates?
3. How long would a replacement take to order, set up and migrate?

Then plan the replacement on your schedule, around your slow season, instead of the server's.

What computers do engineers, schedulers and shop floor users need?

- **Engineers in CAD:** workstation-class machines with dedicated graphics, plenty of memory and fast storage
- **Schedulers, buyers and office staff:** reliable business computers with dual monitors
- **Shop floor stations:** durable, locked-down computers that do one job well
- **Warehouse users:** scanners and tablets built for drops and dust

Then plan replacements on a schedule instead of waiting for failures. A computer that dies mid-shift costs far more than the computer.

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 production.

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 manufacturer with real infrastructure, 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, a network refresh, a plant expansion or compliance readiness work 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.

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 production?

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, including ERP, shipping and production floor connections
2. A coordinated handoff from your current provider. Nobody flips a switch on a Friday afternoon.
3. Changes scheduled around shift changes, month-end and your busiest shipping days
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. Every shift 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 manufacturers, one internal hire is the riskier choice. One person can't be an expert in networks, servers, security, ERP and compliance at once, can't cover two shifts, 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, including on second shift?

A good answer: A specific average they track and report, plus a clear process for urgent issues after hours. 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 Have you connected production equipment like CNC machines to a network?

A good answer: Specific examples, a plan for segmenting production systems, and how they work with equipment vendors.

4 Which ERP and manufacturing systems do you support today?

A good answer: Names you recognize, like Epicor, JobBOSS or NetSuite, without you having to explain them.

5 Who owns a problem between you and our ERP 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 Can you help with NIST 800-171, CMMC and customer security questionnaires?

A good answer: A clear explanation of where the requirements stand today and how readiness work is scoped.

8 What does onboarding look like, step by step?

A good answer: A documented plan built around your production and shipping schedule, 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 manufacturing 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, help integrating equipment like CNC machines, 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 or purchase order. 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 supplier'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

IT outage playbook for production and shipping

Fill in

Fill this in once, review it twice a year, and keep a printed copy where shift leads can find it. When systems go down, nobody should be guessing.

Plant or site	Outage lead	Backup lead	IT support phone

System	What stops without it	Longest we can live without it	Manual workaround
ERP / MRP	Order entry, scheduling, picking		
Shipping and label printing	Labels, bills of lading, carrier pickups		
Internet	Cloud apps, email, remote access		
File server and engineering files	Drawings, programs, work instructions		
Production equipment network	Programs to machines, monitoring		
Phones and email	Customer and supplier contact		

Before an outage

- ☐ Keep a printed contact list for customers, carriers and key suppliers
- ☐ Keep blank shipping labels and manual bill of lading forms on hand
- ☐ Test the backup internet connection and battery backups quarterly
- ☐ Confirm the ERP backup restores (last test date: _____)

During and after

- ☐ Call the outage lead and IT support, and note the start time
- ☐ If ransomware is suspected, unplug the network cable but leave the computer on
- ☐ Tell customers with shipments due today before they call you
- ☐ Afterward, enter manual work into the ERP and update this playbook

Tool 3

Employee offboarding checklist

Print and use

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

Name	Role and shift	Last day	Completed by

Before the last day

- [ ] List every system they use: email, Microsoft 365, the ERP, shipping software, supplier and customer portals
- [ ] List shared logins they know: shop floor stations, shared mailboxes, equipment and vendor portals
- [ ] Move ownership of their files, folders and shared links to their manager
- [ ] List every company device they have, including scanners and tablets

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 ERP, shipping system and portal access
- [ ] Remove any purchasing, banking or payment approval authority
- [ ] Change shared passwords and shop floor logins they knew, and door, gate and alarm codes
- [ ] Collect the laptop, phone, scanner, tablet, keys, fobs and badges
- [ ] Give their manager access to their email and files

Within a week

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

Tool 4

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** customer drawings or specifications, pricing or quotes, anything controlled under ITAR or defense contracts, employee personal information, passwords, or anything covered by an NDA.
3. **Always review** AI output before it goes to a customer, a supplier or the shop floor. 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 work instructions and standard operating procedures
- Summarizing long specs or customer requirements
- First drafts of quotes and customer emails
- Turning meeting notes into action items

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?
- Is it approved for controlled or customer data, if we need it to be?
- What happens to our data if we cancel?

Tool 5

Insurance and customer questionnaire prep sheet

Print and use

Carriers and customers ask about the same controls. Gather the proof once, keep it current, and every application and questionnaire gets easier.

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 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
Network segmentation	Are production systems separated from the office network?	A network diagram showing the separation	☐ 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
Controlled data	Do you handle CUI, and is NIST 800-171 in place where required?	Your system security plan and plan of action, if applicable	☐ 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 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 and your contracts require.

Next step

What happens in a Fairoaks IT assessment

We look at your technology the way a good quality engineer looks at a process: 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 closets, firewall and Wi-Fi, including plant and warehouse coverage
- Servers and your ERP setup
- Microsoft 365 and email security
- Backups, and whether they can actually be restored
- Security tools and updates
- Production equipment connections and segmentation
- Printers, scanners and shipping stations
- Customer, 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 manufacturers 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

"Fairoaks IT truly knows all of us by name and what we do. They even became very familiar with our manufacturing processes and machines in order to truly understand our environment."

Dave Devine
Pierce Aluminum Company

"Fairoaks IT has provided KPM the feel of a friendly internal IT resource that everyone knows but with the breadth of knowledge that comes from having multiple technicians with decades of experience... As we grow, Fairoaks IT adapts."



Winston Anderson
Global Information Systems Manager, KPM Analytics

"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

"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 company, your plant 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/manufacturing-it

Fairoaks IT
Cybersecurity | AI Advisory | Managed IT | Cloud

Soteria Award winner: Most Trusted MSP in North America

© 2026 Fairoaks IT.