contact@namiq.io · namiq.io

NamiQ

NAMIQ GUIDE

Setting Up IT for a Small Firm

Six decisions for a firm of five to fifty with no IT person, each with a check you can run yourself

For the owner or office manager. What unplanned IT costs you, what to do, the questions to put to whoever looks after it, and the templates to start this week.

PREPARED BY	Hung Le, NamiQ	DATE	31 October 2026
FACTS AS OF	31 October 2026	EDITION	1.0
FOR	Owners and office managers	INSIDE	6 decisions, 8 appendices, 5 figures

NamiQ © 2026 NamiQ. All rights reserved. This guide may be shared unaltered, with attribution. Free to read and share.
Web edition: namiq.io/resources/sme-it-infrastructure

START HERE

Six decisions on a page

IT that nobody planned costs a firm a slow leak and, now and then, one event that closes it. Six decisions cover most of both. None needs a full-time hire, and each ends in a check you can run yourself.

Six decisions, each with the first move and a proof you can run yourself.

#	Decision	What it costs you today	First move	Proof it worked	Ch.
1	**Work from anywhere without copying files around**	The meeting that ends "I will send it over"; the private copy nobody else has	Decide, system by system, whether it is a cloud workspace or a VPN	Open yesterday's file from outside the office and see the same version a colleague sees	2
2	**An office network that keeps up with large files**	Minutes of waiting several times a day, and local copies as the response	Wire the seats that move large files	The same large file, timed from a cabled and a wireless seat, before and after	3
3	**Standardised internet access (filtering)**	Bandwidth lost to advertising and tracking, and one way a mistaken click ends badly	Point the office network at a filtering resolver and turn on the categories that matter	A report of last week's blocked requests, shown by your provider	4
4	**Licences paid for use, not headcount**	Eight seats of everything, and a renewal for somebody who left	List each tool, who opens it, and the vendor's licence models today	Every renewal in the next sixty days has a named, current holder	5
5	**Something watching, and a person reading it**	Finding out from a customer three weeks late	Ask who reads the alerts, how fast, and what happens at two in the morning	Last month's alert, who read it and what was done	6
6	**One account per person, and a ten-minute leaver**	"Probably somebody" still has access	One account each, two-step verification on, shared logins listed	Offboard a test account in ten minutes; nothing still lets it in	7

Where to start, for what you have today

You have ten minutes	Page 2, then Chapter 8 for the order, then the six names and dates in 8.3
You want to know what your IT costs you	Chapter 1.3: count the leak for a week
Somebody is about to quote you for something	Appendix D, and Chapters 4 and 6 for the two you will be sold
Somebody is leaving	Appendix B, the ten-minute offboarding checklist
You do not trust your backups	Appendix C, the restore test
You want to stop overpaying for software	Chapter 5 and Appendix E
You want it done for you	The asset review, Chapter 8.2

Edition 1.0, 31 October 2026. The only figures in this guide are two published studies, with their scope stated, and the times you measure yourself.

Contents

How to use this guide 4
1. Why this is worth an afternoon 5
2. Working from anywhere, properly 6
3. The office network, and why large files punish a cheap one 7
4. Standardised internet access: faster and safer are the same job 8
5. Licences: the money most small firms leave on the table 9
6. Something watching, and a person reading it 10
7. Accounts, identity and the leaver problem 11
8. The order to do it in 12

APPENDICES

Appendix A. The inventory sheet 14
Appendix B. The ten-minute offboarding checklist 14
Appendix C. The restore test 14
Appendix D. Questions to ask a provider 15
Appendix E. The licence inventory 15
Appendix F. The monthly thirty-minute review 15
Appendix G. Glossary 16
Appendix H. Sources, and what this guide does not claim 16

How to use this guide

Nobody planned your IT. It accumulated: a router from the internet provider, a shared drive somebody set up, licences bought one at a time as people joined, and a server in the corner that a contractor built and nobody has logged into since. It works, mostly. This guide is what it costs you that it works mostly, and the six decisions that would change it.

It is written for the owner or office manager of a firm of five to fifty that has no IT person. You do not need to know what a VLAN is. Every chapter opens with what the problem costs you today, says what to do, and ends with two things you can use without us: the questions to put to whoever looks after your IT, and a way to check, yourself, that it worked.

Read page 2 first. It is the whole guide on one page, with the first move for each decision. If you only do the first two things in Chapter 8, you will have removed most of the risk that actually closes small firms.

The order to do it in. If you only do the first two, you remove most of the risk that closes small firms.

1
Find out what you have
a week

2
Restore a backup in front of somebody
cheap, and it changes minds

3
One account each, two-step on
free or close to it

4
The network: cables, access points, filtering
the one people thank you for

5
The licence inventory
often pays for the steps above

6
Then monitoring
last, so it watches a tidy estate

How the guide is laid out

Chapter	The decision	What it fixes
1	Why this is worth an afternoon	The slow leak, and the one cost that arrives all at once
2	Working from anywhere	The meeting that ends with "I will send it over"
3	The office network	Large files that crawl, and a version problem on top
4	Standardised internet access	Bandwidth lost to advertising, and one way a mistaken click ends badly
5	Licences	Paying for headcount instead of use, and renewals for people who left
6	Something watching	Finding out from a customer three weeks late
7	Accounts and the leaver problem	"Probably somebody" still has access
8	The order to do it in	What to do first, and what to leave until last
Appendices A to H	Templates and checklists	An inventory, an offboarding list, a restore test, questions for a provider, a licence sheet, a monthly review, a glossary, the sources

What this is not

It is not a product and it does not need one. If you take all of it, hand it to your existing provider and never speak to us, the guide has done its job. It is not a measurement of your firm: we have not measured your network, your licences or your time, and the guide says so wherever a number would otherwise tempt you. And it is not advice on any one product; where a choice depends on what you run, it tells you what to ask.

Conventions

- Words you will meet on a quote, such as VPN, SIEM and XDR, are explained in Appendix G the first time they matter and again at the back.
- "Your provider" means whoever looks after your IT today: a contractor, a supplier, a member of your own team or you.
- A "proof" is something you can do yourself, in front of somebody, that shows a decision has taken effect. A report saying it has is not a proof.
- Nothing here quotes a price. Costs are in time, errors and risk.

1. Why this is worth an afternoon

YOU WILL	see what unplanned IT costs a firm like yours, and why the cost never appears on a bill.
KEY IDEA	the expensive part is a slow leak you do not notice, and one sudden event that closes firms.
TEN MINUTES	count your own leak for a week, with the sheet in section 1.3.

1.1 The leak

The cost of unplanned IT is almost never a bill. It is a slow leak: the minutes a file takes to open over the wrong connection, the afternoon lost when someone works from home and cannot reach the drive, the licence renewed for a person who left, the hour your most capable employee spends being the IT department instead of doing the job you hired them for.

None of those show up anywhere you would notice. They come out of the people you can least afford to lose time from, and they are quiet enough that nobody puts them on a list.

1.2 The event

The other cost arrives all at once, and it is the one that closes firms: the ransomware that spreads because everyone is an administrator, the backup that turns out never to have been restored, the client questionnaire you cannot answer that stalls a contract you had already won.

Six decisions cover most of both. None of them is exotic and none requires a full-time IT hire.

1.3 Put a number on your own leak

We have not measured your firm, and we will not guess a figure for it. You can measure it in a week. Ask everyone to put a mark on a shared sheet each time one of these happens, with the minutes it cost:

What happened	Minutes lost	Who
Waited for a file to open or save		
Could not reach something from home or a client site		
Asked a colleague (not a provider) to fix an IT problem		
Could not do something because a licence or login was missing		

At the end of the week add the minutes, multiply by the number of working weeks in a year, and compare it with the hours you would spend on the first two steps in Chapter 8. That comparison is the real case for an afternoon, and it is yours, not ours.

1.4 Ten minutes: start the sheet

Make the sheet, send it to the team today, and put a reminder in the calendar for one week from now.

2. Working from anywhere, properly

YOU WILL	choose, system by system, whether people reach it through a cloud workspace or a VPN, and know when neither is right.
KEY IDEA	the goal is one copy of every file. Remote access that depends on copying files around creates the copy nobody else has.
PROOF IT WORKED	from outside the office, open yesterday's file from a phone or laptop and see the same version your colleague sees.

2.1 What it costs you today

Someone is at a client site and cannot open the file they need, so the meeting ends with "I will send it over" and the decision waits a day. Someone works from home and emails themselves a copy to work on, which becomes the version nobody else has. Both are the same missing thing.

2.2 What to do

Remote access that does not depend on copying files around. In practice it is one of two shapes: everything the business works on lives in a cloud workspace and is reachable from anywhere by design, or a VPN connects a laptop back to the office network so the shared drive behaves the same from a kitchen table as from a desk.

Two shapes of remote access. Decide which one each system is in.

A cloud workspace

Everything the business works on lives in one workspace and is reachable from anywhere by design.

Good for: documents, mail, shared files.

A VPN

A laptop connects back to the office network, so the shared drive behaves the same from a kitchen table as from a desk.

Good for: things that have to stay in the building.

Neither fits software that keeps a live shared model or database open over the network (design and engineering tools in particular). That case needs the vendor's own collaboration service.

Most firms end up with both: cloud for documents, a VPN for the things that have to stay in the building. The decision worth taking deliberately is which category each system is in, because the answer drives the backup plan, the access list and the cost.

2.3 One caveat before somebody sells you the wrong thing

A VPN is right for reaching files and applications. It is the wrong answer for software that keeps a live shared model or database open over the network, design and engineering tools in particular, because those were built assuming a fast local connection and behave badly across a slow one. That case needs the vendor's own collaboration service instead. A provider who proposes "VPN to the file server" for everything has not asked what you run.

The outcome: the same working day wherever it happens, and one copy of every file.

2.4 Ask your provider

- For each system we use, is it reached through a cloud workspace or a VPN, and why that one?

- Which of our applications keep a live shared model or database open, and what does the vendor offer for working remotely with it?
- If the VPN is down, what can people still do, and who is told?

2.5 Check it worked

Pick a file that was saved yesterday. From a phone on mobile data, or a laptop away from the office, open it. Ask a colleague in the office to open the same file. Check that you both see the same last-saved version, and that you did not have to email anything to yourself. If you did, the decision is not made yet.

3. The office network, and why large files punish a cheap one

YOU WILL	wire the seats that move large files, replace a consumer router with proper access points, and separate guests and devices from client work.
KEY IDEA	for work with large files the network is a productivity tool, not plumbing, and a slow one makes people keep private copies.
PROOF IT WORKED	time the same large file from a cabled seat and a wireless seat, before and after, and write both times down.

3.1 What it costs you today

If your work involves large files, such as drawings, models, video, scans or photography, the office network is a productivity tool, not plumbing. A 2 GB file over a saturated wireless connection is minutes of waiting, several times a day, per person. People respond by keeping local copies, and now you have a version problem as well as a speed problem.

3.2 What to do

Three unglamorous things, in this order:

- **Wire the heavy seats.** Anyone moving large files or driving a graphics-heavy application should be on a cable, not wifi. It is the single cheapest speed improvement available and it is usually a morning's work.
- **Business access points, not a provider's router.** A consumer router doing the job of an office network is the most common thing we find. Proper access points cover the space evenly, hand a laptop over cleanly as someone walks, and separate the staff network from the one you give visitors.
- **A separate network for guests and devices.** Visitors, phones, the printer and anything smart belong away from the machines holding client work. It is one setting on the right equipment and it limits how far a problem on any of them can travel.

Why the heavy seats go on a cable.

Wireless seat	Laptop ▶ Shared wireless ▶ Access point ▶ Switch ▶ File server	The air is shared and varies. Large files wait.
Cabled seat	Laptop ▶ Cable ▶ Switch ▶ File server	A dedicated path. The disk sets the speed.

Separately: guests, phones, the printer and anything smart sit on their own network, away from the machines that hold client work.

The outcome: large files open at the speed the disk can manage rather than the speed the wifi allows, and collaboration happens on one copy because working on one is no longer slower than keeping your own.

3.3 Ask your provider

- Which of our seats move large files, and are they on a cable?
- What equipment carries the wireless, and is it the equipment the internet provider supplied?
- Which networks do visitors, phones, the printer and smart devices sit on, and can any of them reach the file server?

3.4 Check it worked

Choose one large file (about a gigabyte or more) and a shared folder. From a cabled seat, copy it to the folder and note the minutes. Repeat from a wireless seat. Do it again after the change. Keep the four numbers on the inventory sheet in Appendix A. The change is real if the wireless time falls and the two seats stop being very different.

3.5 Ten minutes: find your heavy seats

List the people who open files bigger than a gigabyte, and next to each write whether they are on a cable.

4. Standardised internet access: faster and safer are the same job

YOU WILL	point the office network at a filtering resolver once, for every device, and know what to turn on and what to leave alone.
KEY IDEA	deciding which addresses the office may reach removes advertising and known-bad sites before they are requested, so it is a speed gain and a security control at once.
PROOF IT WORKED	your provider shows you the categories that are on and a list of what was blocked last week.

4.1 What it costs you today

A meaningful share of what your connection carries is advertising and tracking that nobody in the building wanted. It uses bandwidth you paid for and it makes every page slower to load, which is a small tax collected many times a day.

Filtering at the network level, deciding which addresses the office is allowed to reach, once, for every device, removes most of it before it is ever requested. The same mechanism blocks known phishing and malware sites, which is why this is a security control and a performance improvement at the same time.

4.2 What the research says, and what it does not

Two published studies put a number on the first half:

Finding	Source
25 to 40% less network traffic with ads blocked: 25% on ordinary browsing, 40% where streaming video is involved	Simon Fraser University (reported by VentureBeat)
25 to 34% reduction in data transferred, averaged across the major blockers	A peer-reviewed measurement study (arXiv 1705.03193)

Both figures measure browser ad blocking on consumer web browsing. Network filtering in an office is the same mechanism against a different mix of traffic: if most of your bandwidth is project files, the share you recover is smaller. We quote the studies rather than a number of our own because we have not measured your network.

4.3 What to do

Point the office network at a filtering resolver, turn on the categories that matter (advertising, tracking, known malicious and phishing domains) and leave the rest alone. Resist the temptation to block categories on grounds of productivity: it generates arguments, people route around it, and it buys nothing.

The outcome: a connection that carries your work instead of somebody else's advertising, and one fewer way for a mistaken click to end badly.

4.4 Ask your provider

- Which filtering service does the office use, and which categories are on?
- Does it apply to every device on the office network, including phones and guests, or only to the ones someone configured?
- Can you show me last week's blocked requests, and who looks at them?

4.5 Check it worked

Ask your provider to show the settings and a report of blocked requests for the last seven days. A report with real entries is the proof. A setting with no report behind it is a setting nobody has looked at.

5. Licences: the money most small firms leave on the table

YOU WILL	make an inventory of what you own, who opens it, and which licence model each vendor sells today, and tie every licence to a named person.
KEY IDEA	a pool sized to how many people work at once is usually smaller than your headcount, where a vendor offers one.
PROOF IT WORKED	every renewal in the next sixty days has a named person who still works here and still opens the tool.

5.1 What it costs you today

Specialist software is usually bought one seat at a time, as people join, on whichever plan was in front of whoever bought it. Nobody revisits it. So a firm of eight ends up paying for eight of everything, including tools that two people open once a month, and for at least one seat belonging to somebody who left.

5.2 What to do

Find out which of your tools support floating licences: a shared pool where a licence is checked out while someone is using it and returned when they close the application. Where a tool offers it, a pool sized to how many people actually work at once is usually smaller than your headcount, and the saving is immediate and permanent.

Named seats, or a pool. An illustration, not your numbers.



Shaded: in use at this moment. Not every vendor offers a pool; the guide's work is the inventory.

Not every vendor offers it, and the landscape changes: several have moved from network licensing to named users in recent years, and some of those offer a token or pay-as-you-go plan for occasional users instead. The work is an inventory: what you own, who actually opens it, and which model each vendor sells today. It is usually an afternoon, and Appendix E has the sheet.

While you have the list open, tie each licence to a person in your account records. It is the only way the renewal for a leaver ever gets cancelled.

The outcome: you pay for concurrent use rather than headcount, and no renewal outlives the person it was bought for.

5.3 Ask your provider

- Which of our tools offer floating or token licences today, according to the vendor's current terms?
- Who last opened each tool, and who is the named holder of each seat?
- Which renewals fall in the next sixty days, and has anyone checked they are still needed?

5.4 Check it worked

Fill in the sheet in Appendix E. Sort by renewal date. For each renewal in the next sixty days, the "named holder" must be a person who still works here and who opened the tool in the last ninety days. Anything that fails is either a cancellation or a conversation.

5.5 Ten minutes: find the leaver's seat

Pick the last person who left. Search your renewals for anything bought in their name. If you find one, you have found the first saving.

6. Something watching, and a person reading it

YOU WILL	know what a SIEM and XDR are only well enough to read a quote, and ask the questions that matter: who reads the alerts, how fast, and what happens at two in the morning.
KEY IDEA	a new deployment is noisy for weeks, and tuning that noise down is most of the work. Anyone promising a quiet console on day one is describing a demo.
PROOF IT WORKED	your provider shows you last month's alert, what it was, who read it and what was done.

6.1 What it costs you today

Most damage to a small firm is not discovered by the firm. It is discovered by a customer, a bank, or the morning everything stops. The gap between something starting and somebody noticing is usually measured in weeks, and almost everything that makes an incident expensive happens inside that gap.

6.2 What to do

Collect the signals your systems already produce (sign-ins, laptops, servers, email and cloud accounts) into one place that can raise a flag. The tooling for the collecting is a SIEM; extending it past the network to the devices and accounts themselves is what the industry calls XDR. Both are worth knowing only because you will see them on a quote.

6.3 What nobody will tell you when they sell it

A new deployment is noisy for the first few weeks, and tuning that noise down is most of the work. Anyone promising a quiet console on day one is describing a product demo. The question to ask a provider is not what their tool detects. It is who reads the alerts, how quickly, and what happens at two in the morning.

The outcome: somebody finds out the day something changes, instead of a customer telling you three weeks later.

6.4 Ask your provider

- Who reads the alerts, by name or by role, and during which hours?
- How quickly is a serious alert looked at, and what happens outside those hours?
- Can you show me the last alert that mattered, what it was and what was done about it?

6.5 Check it worked

Ask for last month's alerts. A good answer is a short list with a name and an action against each. A warning sign is "nothing happened", with no list, or a list nobody has read.

7. Accounts, identity and the leaver problem

YOU WILL	put one account per person at the centre, connect everything that can connect to it, and make leaving a ten-minute job.
KEY IDEA	you cannot remove a person in one place if logins were created tool by tool. Two-step verification, no shared logins and ordinary users all follow from one account each.
PROOF IT WORKED	offboard a test account in ten minutes and check that nothing still lets it in.

7.1 What it costs you today

Ask who still has access to something and most firms answer "probably somebody". That is not carelessness. It is what happens when logins were created tool by tool over several years, because there is no single place to remove a person from.

7.2 What to do

Put one account per person at the centre, a company identity through your email and document provider, and connect everything that can connect to it. Four things follow, and none of them is possible without it:

- **Removing access in one place** when somebody leaves, rather than in twelve, from memory, on their last afternoon.
- **Two-step verification everywhere at once.** The cheapest control there is, usually free, and the first line of every client security questionnaire.
- **No shared logins.** A shared account for a licence portal or the bank is normal and understandable, and it is why nobody can say who did what, and why one person leaving means changing a password for everyone.
- **Ordinary users, not administrators.** If everyone can install anything, a bad click reaches everything. This is the setting most likely to annoy people if it is changed badly, so it is worth agreeing rather than imposing.

Leaving, with and without one account at the centre.

Tool by tool	One account at the centre
Many logins, created one by one over the years. On the last afternoon someone removes the person from each, from memory.	Switch the person off once. Email, files, applications and sessions that connect to it go with it.
Result: "probably somebody" still has access.	**Result: a ten-minute offboarding that works.**

Encrypt the laptops while you are here. It is already built into the machines you own and usually just not switched on, and it is the difference between losing a laptop and telling your clients you lost their files.

The outcome: a ten-minute offboarding that actually works, and an honest answer when someone asks who can reach what.

7.3 Ask your provider

- Is there one account per person that we can switch off in one place, and what does that switch off?
- Is two-step verification on for every account, including the owner's and the administrators'?
- Which logins are shared, and who knows the passwords?
- Are the laptops' disks encrypted, and can you show me?

7.4 Check it worked

Create a test account, give it the access a new starter would have, then run the offboarding checklist in Appendix B and time it. Afterwards try to sign in as that account, and to open a shared file. Ten minutes and no access is the proof. Anything still working is where the leaver problem lives.

7.5 Ten minutes: list the shared logins

Write down every login more than one person uses, and who knows the password. That list is the first thing to remove.

8. The order to do it in

YOU WILL	do the six decisions in the order that cuts cost and risk fastest, and know what to leave until last.
KEY IDEA	not all six at once, and not in the order a vendor would like. Restoring a backup in front of somebody is the step that changes minds.
TEN MINUTES	write a name and a date beside each of the six steps.

8.1 The sequence

Cost and risk both fall fastest in roughly this order:

1. **Find out what you have.** Every machine, service and account; what is exposed; who can reach what; and whether the backups restore. Everything below is guesswork without it, and it is usually a week. Appendix A has the sheet.
2. **Restore a backup in front of somebody.** Not a report saying backups ran. An actual file, recovered, watched. This is the one that changes minds, and it is cheap. Appendix C has the test.
3. **One account each, with two-step on.** Free or close to it, and everything else in access control depends on it.
4. **The network:** wire the heavy seats, put in real access points, turn on filtering. The fastest visible improvement, and the one people thank you for.
5. **The licence inventory.** Often pays for the steps above.
6. **Then monitoring.** Last, because watching an estate you have not tidied generates alerts about problems you already knew you had.

If you only ever do the first two, you will have removed most of the risk that actually closes small firms, and you will know enough to argue with anybody who quotes you for the rest.

8.2 Where to start

If you want to know where you stand before doing anything, our five-question check takes a minute and answers back immediately, and the full questionnaire covers everything in this guide. Both are free, at namiq.io/managed-it. If you would rather have somebody do the first step with you, the asset review is the first step in this chapter, done for you: every machine, service and account; what is exposed; who can reach what; and whether the backups restore. You keep the inventory whether or not we do anything else, and if the answer is that you are in better shape than you feared, that is the answer you get.

8.3 Ten minutes: put names and dates on the six steps

Copy the six steps onto a page. Beside each, write who will do it and by when. A step with no name will not happen.

APPENDICES

Appendix A. The inventory sheet

Chapter 8, step one. Make one row for every machine, service and account. Do not try to be complete in one sitting: a first pass with gaps is more useful than a perfect one next quarter.

Item	What it is for	Who owns it	Where it lives	Who can reach it	Backed up?	Restore tested (date)

What to record, by kind.

- **A machine** (laptop, desktop, server, network device): the person who uses it, what it holds, whether its disk is encrypted, and the last date it was updated.
- **A service** (email, file storage, the accounting package, the design software's licence server): who administers it, who is billed, how people sign in.
- **An account:** the person, what it can reach, whether two-step verification is on, and whether it is shared. A shared account gets a second row naming everyone who knows the password.
- **Timings from Chapter 3.** The time to copy a large file from a cabled seat and from a wireless seat, with the date.

Appendix B. The ten-minute offboarding checklist

Run it when somebody leaves, and run it once on a test account (Chapter 7.4). The point is that every step is in one place.

1. **Switch off the company account** at the centre (the identity behind email and documents). Note the time.
2. **End the sessions.** Sign the person out of everything that is still open, and remove saved sign-ins on any device they keep.
3. **Remove them from shared drives, groups and distribution lists.** Decide who takes over their files and their mail, in writing, before the last day.
4. **Take back the laptop and phone.** Record who has them, then wipe and reassign, or keep them as a spare.
5. **Cancel or reassign their licences** (Appendix E). A renewal in a leaver's name is a saving.
6. **Change every shared password they knew,** then plan to remove the shared logins (Chapter 7.2).
7. **Record it:** the date, who did it, and what was left for later.

Afterwards, try to sign in as the leaver and to open a shared file. If either works, the checklist has a gap.

Appendix C. The restore test

Chapter 8, step two. Do it in front of somebody, once now and every quarter after.

1. **Choose a real file,** one that matters and is not in the folder everybody opens. Write down its name, where it lives, and when it was last changed.
2. **Ask your provider to restore it** to a different place, from the backup, not from the live copy.
3. **Time it** from the request to the file being open on your screen.
4. **Open it** and check that it is the right version and that nothing is missing.
5. **Record the result:** the date, the file, how long it took, who did it.

6. **If it fails,** that is the finding, and it is the most valuable thing the test can tell you. Write down what failed and by when it will be fixed, and run it again.

A report that backups ran is not a restore test. An actual file, recovered, watched, is.

Appendix D. Questions to ask a provider

One page to take into the room. A good answer is specific and can be shown. A warning sign is an answer that is a promise with nothing behind it.

Topic	Ask	A good answer sounds like	A warning sign sounds like
Remote access	For each system we use, is it a cloud workspace or a VPN, and why?	A list by system, with a reason for each	"A VPN for everything"
Large files	Which of our seats move big files, and are they on a cable?	Names of seats, a cable plan	"The wifi is fine"
Network	What carries our wireless, and which network do guests and devices sit on?	Business access points, guests and devices on a separate network	"The router from the internet provider"
Filtering	Which categories are on, for which devices, and can I see last week's blocks?	A category list and a real report	"It is switched on" with no report
Licences	Which tools offer floating or token licences today, and who holds each seat?	A sheet with named holders and renewal dates	"We renew what we had"
Monitoring	Who reads the alerts, when, and what happens at two in the morning?	A role, hours, a response time, a named escalation	"The tool detects everything"
Accounts	Can we switch off one account and lose everything for a leaver, and is two-step on for all?	Yes to both, with a demonstration	"We change the passwords"
Backups	When did you last restore a file in front of us?	A date, a file and a time taken	"The backups ran last night"
Support	Where does the team send a request, and does every reply carry a ticket number?	One place, a number, a link back	"Just call whoever you know"

Appendix E. The licence inventory

Chapter 5. One row per tool. "Named holder" must be a person who still works here.

Tool	Vendor's licence models today	Seats we pay for	People who opened it in the last 90 days	Named holder	Renewal date	Action

Reading it. A tool with more seats than people who opened it is a candidate for a smaller or floating arrangement, if the vendor offers one. A seat with no named holder, or a holder who left, is a cancellation. A renewal inside sixty days with an action still blank is the next thing to deal with.

Appendix F. The monthly thirty-minute review

Put it in the calendar, name the person and a deputy. It is short on purpose.

1. **Joiners and leavers.** Does every person who joined or left this month have an account state that matches? Did anyone run the offboarding checklist?
2. **Renewals.** Anything renewing in the next sixty days, with a named holder who still needs it?
3. **A file restore.** One file, recovered and opened. Note the date.
4. **The alerts.** Who read last month's, and what was done?
5. **Shared logins.** Has anyone added one? Can it be removed?
6. **Anything new.** A device, a service or an account that is not on the inventory sheet goes on it today.

Appendix G. Glossary

Access point. The device that gives laptops and phones a wireless connection to the office network. A business access point covers a space evenly and separates staff from guests; a consumer router does both jobs badly.

Floating licence. A shared pool of licences: one is checked out while someone is using the software and returned when they close it. Compare a named-user licence, tied to one person.

Filtering resolver. The service the office network asks to find a website's address. A filtering one refuses addresses for advertising, tracking and known-bad sites.

Offboarding. Everything done when a person leaves so that they can no longer reach anything.

Ransomware. Software that locks a firm's files and demands payment to unlock them. It spreads further when many people are administrators.

SIEM. A system that collects the signals your systems already produce, such as sign-ins and device events, into one place that can raise a flag.

Two-step verification. A second proof, usually a code or an approval on a phone, in addition to a password.

VPN. A private connection from a laptop back to the office network, so the shared drive behaves the same from anywhere.

XDR. The same idea as a SIEM, extended from the network to the devices and accounts themselves.

Appendix H. Sources, and what this guide does not claim

Sources.

- Simon Fraser University study of the network traffic saved by blocking ads, reported at venturebeat.com/business/blocking-ads-can-cut-network-traffic-25-to-40-study-shows
- A peer-reviewed measurement study of data saved by browser ad blockers: arxiv.org/pdf/1705.03193

What this guide does not claim.

- It does not measure your firm. The only figures in it are two published studies, with their scope stated, and the times you measure yourself.
- It does not say any product is the right one. Where the answer depends on what you run, it gives you the question.
- It does not say that doing the six decisions makes a firm safe. It says what removes the risks that most often close a small firm, in the order that does it fastest.