



EngineerAustin

## A PRACTICAL CHECKLIST FOR OWNERS

# Questions to Ask Your IT Provider

Whether your IT is in-house, outsourced or a mix, these questions show how healthy your systems are and how well they are being run.

Tick each question once you have a clear answer. A good provider will be glad you asked and can usually show you the answer in writing. Anything you cannot get a clear answer to is worth a closer look.

### Who is looking after us?

- ☐ How long have you been in business, and can we speak with current references?
- ☐ Which certifications and training do your technicians hold that are relevant to our systems (e.g., Microsoft, our firewall or network vendor, CJIS)?
- ☐ How do you keep up with new threats and changes in security practice?
- ☐ What is your staff turnover, and who will actually work on our account?
- ☐ Would you welcome a second opinion from an independent site or security assessment?

### Ownership, contract and exit

- ☐ Who owns our Microsoft 365 or Google tenant, our domain name and the administrator passwords: us or you?
- ☐ If we leave, what do we get back (data, credentials, documentation), and how quickly?
- ☐ Are response times written into the contract?
- ☐ Do we receive network diagrams, a device inventory and a written restore procedure that we keep?
- ☐ Can we have a written list of the services you provide and the policies you manage for us?
- ☐ How is **your** remote access to our systems protected, and what happens to it when one of your staff leaves?
- ☐ What is your policy on AI tools that touch our data?

### Backups and recovery

- ☐ Is a copy of our data kept offsite and locked against deletion (immutable)?
- ☐ When was the last test restore, and is the result written down?
- ☐ What are our disaster recovery and business continuity plans, and who has a copy?

### Day-to-day protection

- ☐ What do you do proactively to keep our systems healthy, safe and backed up?
- ☐ Are updates applied on a schedule to computers, servers, firewalls, printers and other network equipment?
- ☐ Is anything past end of support? (Windows 10 support ended October 2025.)
- ☐ Does every computer and server have endpoint detection and response (EDR), not just antivirus?
- ☐ Is multi-factor authentication (MFA) on every account, administrators included, using an authenticator app, with legacy sign-in methods blocked?
- ☐ Do we follow current NIST password practice (long passphrases, no forced periodic changes), and does our staff have a password manager?
- ☐ Is the firewall supported and updated, and are any paid security subscriptions actually active?
- ☐ Is our email filtered, with SPF, DKIM and DMARC set up on our domain and a warning banner on outside mail?
- ☐ Are guest Wi-Fi, smart (IoT) devices, printers and cameras on their own network segments?
- ☐ Is remote access limited to managed devices, with no remote desktop exposed to the internet?
- ☐ What layers of defense protect us, and what happens if one of them fails?

### People, policy and paperwork

- ☐ What is the checklist when an employee joins, changes roles or leaves, on our team or yours?
- ☐ Does our staff get security training every year, including AI-written phishing, cloned-voice calls, QR-code scams and payment-change fraud?
- ☐ How often are we scanned for vulnerabilities, and when would we need a penetration test?
- ☐ Does our cyber-insurance questionnaire match what is actually configured?
- ☐ Which requirements apply to us (HIPAA, PCI, CJIS, Texas SB 2610, the state-required cybersecurity training for Texas public entities), and **who helps us document it?**



EngineerAustin

A BASELINE TO COMPARE AGAINST

# What a Well-Run Small Network Has in 2026

Not every business needs every item, but each one you skip should be a decision someone made on purpose.

Each item below matches a question on the front. If you can tick it and point to where it is written down, you are in good shape.

## Accounts and sign-in

- ☐ **MFA on every account**, administrators and the IT provider included, using an authenticator app rather than text messages, with legacy sign-in blocked.
- ☐ **Current password practice**: long passphrases, checks against known-breached passwords, no forced periodic changes, and a password manager for staff.
- ☐ **Business email on your own domain**, not personal Gmail, Yahoo or Hotmail accounts.
- ☐ **You own the keys**: the tenant, domain and administrator credentials are in the business's name.
- ☐ **A joiner and leaver checklist**, so accounts and access change the same day a role does.

## Computers and devices

- ☐ **EDR on every computer and server**, not just traditional antivirus.
- ☐ **Encryption** on every device that stores client or personal information.
- ☐ **Automatic screen lock** on every computer and phone.
- ☐ **Scheduled updates** for computers, servers, printers and network equipment.
- ☐ **Nothing past end of support**, and a plan for anything getting close.
- ☐ **Device-based access**: only managed, up-to-date devices get full access to company data.

## Network

- ☐ **A supported, updated firewall**, with any paid security subscriptions confirmed active.
- ☐ **Segmentation**: staff, guest Wi-Fi, and IoT devices, printers and cameras each on their own segment.
- ☐ **Business-grade wireless** access points, kept updated.
- ☐ **Secure VPN** for site-to-site links, working from home and travel.
- ☐ **No remote desktop** exposed to the internet.

## Email

- ☐ **Filtering** for spam, malware and impersonation.
- ☐ **SPF, DKIM and DMARC** on your domain, now expected by the large mail providers.
- ☐ **External-sender banners** so staff can spot outside mail.

## Backup and recovery

- ☐ **An offsite copy locked against deletion**, so ransomware or a stolen login cannot erase it.
- ☐ **Test restores** on a schedule, with the date and result written down.
- ☐ **A written disaster recovery and business continuity plan** that more than one person knows.

## People and training

- ☐ **Yearly security awareness training** with phishing exercises.
- ☐ Training that covers **AI-written phishing, cloned voices, QR-code scams and payment-change fraud**.
- ☐ **A call-back rule**: any change to payment or bank details is confirmed by phone at a number already on file.
- ☐ **A written AI policy** on which tools may touch company data.

## Testing and documentation

- ☐ **Vulnerability scans** at least yearly, quarterly where PCI applies.
- ☐ **A penetration test** when an insurer or a framework asks for one.
- ☐ **Documentation you keep**: network diagram, device inventory and restore procedure.
- ☐ **Response times in writing** and clear exit terms with your provider.
- ☐ **Insurance answers that match reality**, reviewed at each renewal.
- ☐ **Your requirements identified** (HIPAA, PCI, CJIS, Texas SB 2610, public-entity training) and the evidence kept in one place.