The SMB IT Readiness Checklist

22 questions every Pittsburgh and Cleveland small business should be able to answer about its technology. Each has a Green, Yellow, and Red answer and one next step. Allow about 20 minutes.

HOW TO USE THIS SHEET

Every question has three answers. Tick the box beside the one that matches your business today: Green means you are in good shape, Yellow is worth fixing soon, and Red should be addressed first.

When you have answered all 22 questions, count the ticks of each color, write the totals on the Score yourself page, and fill in the action plan on the last page.

1. Identity and access

A stolen password lets an attacker straight into your email and files. These four questions come first because the fixes are cheap.

Q1. Is multi-factor authentication required for every user on every business app?

- ☐ GREEN — MFA enforced on Microsoft 365 / Google, VPN, remote access, banking, line-of-business apps, and every admin account. Preferably phishing-resistant (passkeys, FIDO2, or number-matching).
- ☐ YELLOW — MFA on email but not on other apps; or SMS-only MFA (phishable).
- ☐ RED — MFA optional or off.

Next step: Microsoft and Google both include MFA at no extra cost. Turn it on everywhere in the next 30 days.

Q2. Do employees use a password manager, and is password reuse down to zero?

- [ ] GREEN — Company-funded password manager (1Password, Bitwarden, Keeper, Dashlane) with a shared vault, and everyone uses it.
- [ ] YELLOW — Some people use a manager, others reuse passwords or keep them in a spreadsheet.
- [ ] RED — No manager, and a seasonal password like Summer2024 is common.

Next step: Pay for a business plan. Free and personal plans lack recovery, role-based sharing, and audit logs. Budget $4 to $8 per seat per month.

Q3. Is there a formal offboarding process that revokes access within one business day?

- [ ] GREEN — A checklist that disables logins, revokes tokens, forwards email, rotates shared secrets, and collects devices, always done same day.
- [ ] YELLOW — Email and Microsoft 365 shut off, but shared SaaS, VPN, or old tokens linger.
- [ ] RED — Former employees may still have access.

Next step: Build a one-page offboarding checklist this week. Every app your team has ever onboarded someone onto goes on the list.

Q4. Do admin accounts follow least-privilege, and avoid being the same account a person uses to read email?

- [ ] GREEN — Separate admin accounts for domain, Microsoft 365, firewall, and so on. Day-to-day email and browsing use a non-privileged account. PIM or just-in-time access used where possible.
- [ ] YELLOW — Too many people are global admin, or one admin account is used for everything.
- [ ] RED — Everyone is an admin on their own machine, and the owner uses global admin to read mail.

Next step: In Microsoft 365, open Active users, then Admin roles, and trim to a handful of global admins. Create dedicated admin accounts that do nothing else.

2. Backups and recovery

These five questions cover how fast you are back at work if a server, a laptop, or your SaaS data is gone tomorrow morning. Count a backup only after you have restored from it.

Q5. Do you back up your SaaS data (Microsoft 365, Google Workspace, QuickBooks Online)?

- [ ] GREEN — A third-party backup (Datto SaaS Protection, Afi, Dropsuite, Spanning) runs on all SaaS, with a retention policy you reviewed.
- [ ] YELLOW — You assume Microsoft or Google is your backup. Their built-in retention is limited and does not protect you from a deliberate delete.
- [ ] RED — No SaaS backup of any kind.

Next step: Pick any reputable SaaS backup and turn it on this week. Pricing is typically $3 to $6 per seat per month.

Q6. Are your backups stored in at least one location you cannot reach with your regular login?

- [ ] GREEN — You follow 3-2-1: three copies, two media types, one off-site or immutable (S3 Object Lock, Wasabi Immutability, Datto).
- [ ] YELLOW — You have off-site backups but they are reachable with the same admin credentials as production.
- [ ] RED — Backups live on the same server, NAS, or domain as the data they protect.

Next step: Add an immutable or air-gapped destination. An attacker who gets your admin login can delete any backup that login can reach.

Q7. When was your last successful restore test, not just the last backup?

- [ ] GREEN — Within the last 90 days, a real file or VM was restored to verify the backup works.
- [ ] YELLOW — Backups run nightly but no one has actually restored from them in the last year.
- [ ] RED — You are not sure when, or whether, the backups have ever been tested.

Next step: Schedule a quarterly restore test of one critical file, one full machine, and one cloud data set. Put it on the calendar as a recurring task.

Q8. Do you know your RTO (how long you can be down) and RPO (how much data you can afford to lose)?

- [ ] GREEN — Each critical system has a written RTO and RPO, agreed with the business owner, and backups are sized to hit both.
- [ ] YELLOW — You have a sense, but nothing written or verified.
- [ ] RED — Never discussed. In an outage you would improvise.

Next step: Ask each department head: if this were gone at 9am, what is the latest you would need it back? The answers are your RTO. Then check that your backups run often enough to meet each RPO.

Q9. If your primary location lost power and internet for 48 hours, would the business keep running?

- [ ] GREEN — Remote-work-capable workforce, cloud phone system, documented failover steps.
- [ ] YELLOW — Some staff could work remote, but core systems (shared drives, line-of-business app, phones) would be offline.
- [ ] RED — You would stop operating until the site came back.

Next step: Write a one-page continuity plan: who calls whom, what customers hear on the phone, and where staff work from.

3. Endpoint and email security

These five questions cover the devices your team uses and the email that reaches them.

Q10. Does every laptop, desktop, and server run something beyond built-in antivirus?

- [ ] GREEN — Managed EDR (SentinelOne, CrowdStrike, Huntress, or Defender for Business with a human watching alerts) on 100% of endpoints.
- [ ] YELLOW — Defender or other AV is on but no one reviews the alerts.
- [ ] RED — Built-in AV only, or some machines have nothing.

Next step: Inventory every endpoint and confirm modern EDR plus a human on the alerts. Check the servers and the owner's laptop, which are easy to miss.

Q11. Are operating systems and third-party apps patched within a defined window?

- [ ] GREEN — A patch-management tool with a policy: critical patches in 7 days, others in 30, and a monthly compliance report.
- [ ] YELLOW — The operating system auto-updates, but third-party apps (Adobe, Java, browsers) drift.
- [ ] RED — Patches are applied when someone notices.

Next step: Pick a patch-management tool (NinjaOne, PDQ, Intune, Action1) and set a policy. Include browsers and other third-party apps along with the operating system.

Q12. Does inbound email go through a filter that catches phishing and impersonation, on top of the native provider filter?

- [ ] GREEN — Mimecast, Proofpoint, Avanan, IRONSCALES, or similar, with impersonation protection turned on.
- [ ] YELLOW — Default Microsoft 365 or Gmail filter only, and some obvious phishes still reach inboxes.
- [ ] RED — No advanced email filtering; spoofed-CEO emails make it through.

Next step: Turn on the advanced anti-phishing policies your license already includes (Microsoft 365 Business Premium and up), or add a dedicated secure email gateway. Budget $3 to $5 per seat per month.

Q13. Do you have SPF, DKIM, and DMARC set up on your sending domain?

- [ ] GREEN — All three configured. DMARC is at p=reject or p=quarantine, and you monitor the aggregate reports.
- [ ] YELLOW — SPF and DKIM are set, but DMARC is at p=none (reporting only).
- [ ] RED — None of the three set, or SPF has the classic +all or ?all mistake.

Next step: Check your domain at mxtoolbox.com. Without an enforced DMARC policy, other people can send email that appears to come from your domain.

Q14. Is full-disk encryption on every laptop?

- [ ] GREEN — BitLocker (Windows) or FileVault (Mac) enabled on 100% of laptops, with recovery keys escrowed in Entra ID, Intune, or Jamf.
- [ ] YELLOW — Enabled on most laptops but no central recovery key vault.
- [ ] RED — Not enabled, or unknown.

Next step: Anyone who finds an unencrypted laptop can read its files. BitLocker and FileVault are built into Windows and macOS, and one policy turns them on.

4. Network and remote access

These three questions cover the firewall, how the network is divided, and how staff connect from outside the office.

Q15. Is your firewall modern, supported, and reviewed at least yearly?

- [ ] GREEN — A current-generation firewall (Fortinet, Palo Alto, SonicWall, Meraki, OPNsense) with an active license, intrusion prevention on, and rules reviewed annually.
- [ ] YELLOW — A firewall is in place but the license lapsed, and rules have not been reviewed.
- [ ] RED — Consumer router, end-of-life firewall, or default rules never configured.

Next step: A firewall past end of life no longer gets security updates. Confirm the model is still supported and renew the licenses.

Q16. Do guest devices, IoT (cameras, thermostats, printers), and employee laptops live on separate networks?

- [ ] GREEN — Segmented: a production VLAN, an IoT VLAN, and a guest network with client isolation. Printers sit on their own VLAN.
- [ ] YELLOW — A guest network exists but IoT devices share the main network.
- [ ] RED — Everything on one flat network.

Next step: On a flat network a compromised thermostat can reach your file server. With current access points and a managed switch, segmenting a small office takes about an afternoon.

Q17. How do employees connect to work remotely, and is that method safe?

- [ ] GREEN — Single sign-on plus zero-trust access (Cloudflare Access, Tailscale, Twingate) or a modern VPN with MFA. No open RDP to the internet.
- [ ] YELLOW — Legacy VPN with username and password only.
- [ ] RED — RDP or a remote tool exposed to the internet with shared credentials.

Next step: Close any RDP port that is open to the internet today, and move remote access behind a VPN or zero-trust tool with MFA.

5. Incident response and assets

These three questions cover what you do in the first half hour of an incident, whether staff can spot a phish, and whether you know what equipment you own.

Q18. Is there a written incident-response plan that fits on a single page?

- [ ] GREEN — Yes: contacts, a decision tree, who calls the cyber-insurance carrier, who speaks to customers, and where the plan lives. Reviewed annually.
- [ ] YELLOW — A plan exists but nobody has read it in two years.
- [ ] RED — No plan.

Next step: Write the plan on one page with the items listed under Green, keep a printed copy, and review it once a year.

Q19. Have employees gone through phishing-awareness training in the last 12 months?

- [ ] GREEN — Yes, with a reputable platform (KnowBe4, Hoxhunt, Wizer, Curricula), and the failed click-through rate is trending down.
- [ ] YELLOW — One-time training at hire, nothing since.
- [ ] RED — No training.

Next step: Training does not have to be a day-long class. Use five-minute monthly videos with a graded simulated phish.

Q20. Do you have a complete, current asset inventory (who has what laptop, what servers exist, what is in the cloud)?

- ☐ GREEN — An auto-maintained inventory from an RMM or MDM (Intune, NinjaOne, Jamf), updated in real time.
- ☐ YELLOW — A spreadsheet someone updates once a year.
- ☐ RED — You find out what assets you have by looking around.

Next step: Pick an RMM or MDM and let it build the inventory for you.

6. Vendors and documentation

These two questions cover the companies that hold your data and the knowledge that lives in one person's head.

Q21. If a key vendor (accounting platform, file-sharing tool, CRM) had a breach this weekend, would you know what data they hold for you?

- ☐ GREEN — You have a short list of your top vendors, what data each one holds, and a copy of their most recent security report.
- ☐ YELLOW — You trust your vendors but have never asked them anything in writing.
- ☐ RED — You have no list. A vendor breach happens and you find out from the news.

Next step: Pick your three most data-sensitive vendors and ask each for their latest security report. If a vendor cannot produce one, record that as a risk.

Q22. If the one person who knows how all the IT works was out tomorrow, could someone else figure it out?

- ☐ GREEN — The important things (where systems are, how to get in, who to call) are written down somewhere a teammate can find them, and updated when something changes.
- ☐ YELLOW — One engineer or owner is the single point of failure for how everything works.
- ☐ RED — One person knows, and nothing is written down.

Next step: Schedule one hour a month to write down the IT things only one person knows.

Score yourself

Count how many of each color you ticked across the 22 questions and write the totals in the boxes. Then tick the band that matches your result.

GREEN	YELLOW	RED
_____	_____	_____
out of 22	out of 22	out of 22

- [ ] **18 or more Green:** you are in good shape. Keep it that way with quarterly restore tests, monthly patching, and an annual policy review.
- [ ] **11 to 17 Green:** the basics are mostly there. Pick your three most serious Yellows and close them within 90 days.
- [ ] **Under 11 Green, or any Red on Q1, Q5, Q6, Q10, or Q14:** fix any Red on those five questions first, then the rest of your Reds, then the Yellows.

A Red on Q1, Q5, Q6, Q10, or Q14 puts the whole result in the Red band, however many Greens you have.

Action plan

Write down the five things you will fix first. Start with any Red on a critical question (Q1, Q5, Q6, Q10, or Q14), then your other Reds, then your Yellows. Use the next step printed under each question as the starting point.

PRIORITY	WHAT TO FIX	WHO OWNS IT	TARGET DATE	DONE
1				☐
2				☐
3				☐
4				☐
5				☐

Get a second opinion

KawaConnect offers a free IT readiness call to small businesses in Western Pennsylvania and Northeast Ohio. Walk us through your answers and we will tell you what we would fix first and roughly what it costs. For ongoing help, see our managed IT service (kawaconnect.com/managed-it/).

Book a free readiness call: kawaconnect.com/contact/ | sales@kawaconnect.com | (412) 556-7007