FREE RESOURCE · VERSION 1.0

The SMB IT Readiness Checklist

22 questions every Pittsburgh and Cleveland small business should be able to answer about their technology, with a red, yellow, and green rubric and the single next step to take for each one.

~20 minutes
to complete

22 questions
across 6 domains

Scored
so you know what to fix first

HOW THE RUBRIC WORKS

For every question you will see three answer bands. Mark the one that matches your business today.

Green: you are in good shape **Yellow: worth fixing soon** **Red: address this first**

KawaConnect is an IT consulting firm serving Pittsburgh, Cleveland, and the Tri-State area. Questions? Call **(412) 556-7007** or email **support@kawaconnect.com**. No sales pitch inside.

1. Identity and access

Most ransomware in 2025 starts with a stolen password, not a clever exploit. These four questions are first because they are the cheapest fixes with the biggest payoff.

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

Green MFA enforced on M365 / 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: MFA is the single highest-ROI security control. Microsoft and Google both enable it free. 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 "Summer2024!" is a common password.

Next step: Pay for a business plan. Free / personal plans lack recovery, role-based sharing, and audit logs. $4-$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 M365 shut off, but shared SaaS accounts, VPN, or old tokens linger.

Red Former employees may still have access.

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

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

Green Separate admin accounts for domain, M365, firewall, etc. Day-to-day email / browser uses a non-privileged account. PIM / JIT used where possible.

Yellow Too many people are global admin. One admin account is used for everything.

Red Everyone is an admin on their own machine. Owner uses global admin to read mail.

Next step: In M365, run "Active users → Admin roles" and trim to under 4 global admins. Create dedicated *-admin* accounts that do nothing else.

2. Backups and recovery

If a server, laptop, or piece of SaaS data disappears tonight, how fast are you back to work tomorrow morning? Backup-existence questions come before the restore-test question on purpose: a test of nothing is still nothing.

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

Green A third-party backup (Datto SaaS Protection, Afi, Dropsuite, Spanning, etc.) runs on all SaaS, with a retention policy you reviewed.

Yellow You assume Microsoft or Google is your backup (they are not; their retention is limited and does not protect against rogue deletes).

Red No SaaS backup of any kind.

Next step: Pick any reputable SaaS backup and turn it on this week. SaaS backup pricing is typically $3-$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, etc.).

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. Ransomware groups specifically target backups, and a shared credential makes your backup a second target, not a safety net.

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 (M365 or Google Workspace). 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. Stack that against your backup frequency.

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 who? What do customers hear on the phone? Where do staff work from? A bad plan is better than no plan.

3. Endpoint and email security

Q10. Every laptop, desktop, and server runs something beyond built-in antivirus?

Green Managed EDR (SentinelOne, CrowdStrike, Huntress, Defender for Business with a human watching alerts) on 100% of endpoints.

Yellow Defender or other AV is on but no one reviews 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. Servers and the boss' laptop are usually the forgotten ones.

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

Green Patch management tool with policy: critical patches in 7 days, others in 30. Monthly compliance report.

Yellow OS auto-updates, 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. Unpatched browsers are the most common initial ransomware vector.

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 / Gmail filter only, some obvious phishes still make it to inboxes.

Red No advanced email filtering; frequent spoofed-CEO emails make it through.

Next step: Turn on the advanced anti-phishing policies your license already includes (M365 Business Premium and up), or add a dedicated secure email gateway. Budget $3-$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*. You monitor DMARC aggregate reports.

Yellow SPF and DKIM set, DMARC 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. Your failure to publish DMARC is what lets scammers spoof your domain to your customers.

Q14. Is full-disk encryption on every laptop?

Green BitLocker (Windows) or FileVault (Mac) enabled on 100% of laptops, with recovery keys escrowed in Azure AD / Intune / Jamf.

Yellow Enabled on most laptops but no central recovery key vault.

Red Not enabled, or unknown.

Next step: A lost laptop without encryption is a data breach under most state laws. Encrypt today. It is free and takes one GPO or Intune policy.

4. Network and remote access

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

Green A current-gen NGFW (Fortinet, Palo Alto, SonicWall, Meraki) with active license, IPS / IDS on, rules reviewed annually.

Yellow Firewall is in place but license lapsed; rules have not been reviewed.

Red Consumer router, end-of-life firewall, or default-deny rules never configured.

Next step: End-of-life firewalls stop receiving threat intel updates. Confirm the model is still under support and renew licenses.

Q16. Do guest devices, IoT (cameras, thermostats, printers), and employee laptops live on the same network?

Green Segmented: production VLAN, IoT VLAN, guest SSID with client isolation. Printers sit on their own VLAN.

Yellow Guest SSID exists but IoT devices share the main network.

Red Everything on one flat network.

Next step: Flat networks let a compromised thermostat see your file server. Segmenting takes an afternoon with modern APs and a managed switch.

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

Green SSO + ZTNA (Cloudflare Access, Tailscale, Twingate, Perimeter 81) or modern VPN with MFA. No open RDP to the internet.

Yellow Legacy VPN with username / password only.

Red RDP or LogMeIn exposed to the internet, shared credentials.

Next step: Port 3389 open to the world is the single fastest way to get ransomware. Close it today, even if you have to let someone remote in via a phone call.

5. Incident response and training

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

Green Yes: contacts, decision tree, who calls the cyber-insurance carrier, who speaks to customers, where the plan lives. Reviewed annually.

Yellow A plan exists but nobody has read it in two years.

Red No plan.

Next step: The first 30 minutes of an incident decide the week that follows. A single-page plan removes the "what do we do" panic.

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

Green Yes, with a reputable platform (KnowBe4, Hoxhunt, Wizer, Curricula), and failed click-through rate is trending down.

Yellow One-time training at hire, nothing since.

Red No training.

Next step: Awareness does not have to be a day-long class. Five-minute monthly videos with a graded simulated phish are the format that works.

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

- **Green** Auto-maintained inventory from 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: You cannot protect what you cannot list. Pick an RMM or MDM and let it auto-populate.

6. Vendors and documentation

Q21. If a key vendor (your accounting platform, your file-sharing tool, your 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, you find out from the news.

Next step: Pick your three most data-sensitive vendors and ask each one for their latest security report. If they cannot produce one, that is the answer.

Q22. If the one person who knows how all the IT works got hit by a bus tomorrow, could someone else figure it out?

- **Green** The important stuff (where things are, how to get in, who to call) is written down somewhere a teammate can find it. Updated when something changes.
- **Yellow** One engineer or owner is the single point of failure for how everything works.
- **Red** "Jerry knows" is the plan.

Next step: Schedule one hour a month to write down the IT things only one person knows. A boring routine beats a heroic recovery.

Score yourself

Count how many of each color you marked across the 22 questions. Rough interpretation below. It is a starting point, not a verdict.

Green answers	Yellow answers
Red answers	**22** Total questions

18+ Green: you are running a tight operation. The risk now is drift: enforce the cadence (quarterly restore tests, monthly patching, annual policy review).

11-17 Green: the basics are mostly there. Your three biggest Yellows are likely your three biggest risks. Close them in 90 days.

Under 11 Green, or any Red on Q1, Q5, Q6, Q10, or Q14: you have an exposure that turns a routine day into a company-ending event. Treat these as priority one.

Want a second pair of eyes?

KawaConnect runs SMB IT readiness calls free, no pitch. We support businesses across Pittsburgh, Cleveland, and the Tri-State area. Walk us through your answers, we point out what we would fix first and roughly what it costs. No slides, no contract, no follow-up unless you ask.

Call (412) 556-7007 · **Email** support@kawaconnect.com · **Web** kawaconnect.kawalink.us