FREE CHECKLIST · NODEBRIDGE IT

Cybersecurity readiness checklist

Use this simple checklist to see whether your business has the main security basics in place today. It is not a technical audit, but it can help you spot gaps and decide what to fix first.

What this is	A free, plain-language checklist from a matching service — not an IT vendor.
How to use it	Work through each item, jot your answers, and use them to compare providers.
Cost	Free. Matching is always free for businesses.

What this checklist helps you do

Many small businesses know security matters, but are not sure what “good enough for now” looks like. This checklist gives you a practical starting point. It focuses on the basics that reduce common day-to-day risk, like account protection, software updates, backups, and staff habits.

You do not need to be technical to use it. If you can answer yes, no, or not sure for each item, that is enough. “Not sure” is useful. It usually means the process is informal, undocumented, or depends on one person.

This is general educational information, not a security assessment. Requirements vary by industry and state. If you handle health, payment, legal, or other sensitive data, you may have extra rules to follow.

How to use the checklist

Review each item and mark one answer: Yes, No, or Not sure. Be honest. The goal is not a perfect score. The goal is to understand where you are today.

If you are an owner or office manager, you may want to answer with input from whoever handles computers, software, or vendors. Do not send us passwords, network details, or system access. We only ever collect basic business and contact details if you ask us to help you find a provider.

A good rule is simple. If a security step happens only “when someone remembers,” count that as No. If it happens regularly, is written down, and more than one person knows the process, count that as Yes.

The cybersecurity readiness checklist

Score each item as Yes, No, or Not sure.

1. Multi-factor authentication is turned on for email, accounting, banking, file storage, and other important systems. Multi-factor authentication, or MFA, means users need a second step to sign in,

like an app code or security key, not just a password.

2. Each employee has their own account. Shared logins are avoided, especially for email, finance, and admin tools.

3. Former employees and old vendors are removed quickly from accounts, software, Wi-Fi, and devices.

4. Passwords are strong and unique, and your team uses a password manager instead of reusing passwords in a spreadsheet or notebook.

5. Computers, phones, routers, and business apps are updated regularly. Patching means installing security and bug-fix updates so known weaknesses are less likely to be exploited.

6. Antivirus or modern device protection is installed and active on business computers. Endpoint means a device like a laptop, desktop, phone, or tablet that connects to your business systems. EDR, or endpoint detection and response, is a more advanced tool some providers use to spot and investigate suspicious activity on those devices.

7. Important data is backed up automatically, not just copied by hand once in a while.

8. Backups are tested from time to time by restoring a file or system, so you know the backup is usable.

9. Your backup approach roughly follows the 3-2-1 backup rule. That means keeping 3 copies of important data, on 2 different types of storage, with 1 copy kept offsite or in the cloud.

10. Staff know how to recognize suspicious emails, fake invoices, and unexpected login prompts, and they get simple security training at least once or twice a year.

11. There is a clear way for staff to report something suspicious quickly, without feeling embarrassed.

12. Business Wi-Fi is secured, uses a strong password, and guest Wi-Fi is separate from business devices when possible.

13. Admin access is limited to the few people who truly need it. Not everyone should be able to install software, change security settings, or access all files.

14. You know what devices and key software your business relies on. This does not need to be fancy, but there should be a current list.

15. Remote work is handled with basic rules, like screen locks, approved devices, and secure access to files and apps.

16. If you collect card payments, health information, or other regulated data, you know which rules may apply. PCI refers to payment card security requirements. HIPAA is the Health Insurance Portability and Accountability Act, which applies to certain healthcare information in the US. SOC 2 is a reporting standard some software vendors use to show how they handle security controls.

17. You know who to call if something goes wrong, such as a suspicious login, lost laptop, or ransomware event. Even a simple contact list is better than figuring it out during a stressful day.

18. Your main software vendors and IT providers are documented, with current support contacts and renewal dates.

19. If an outside company helps with IT, you understand what they are responsible for and what they are not. An SLA, or service level agreement, is the part of a contract that explains response targets and service scope. RMM, or remote monitoring and management, is software many managed providers use to watch device health, apply updates, and support systems remotely.

20. Security decisions are reviewed at least occasionally, not only after a problem. Some managed providers also offer vCIO support. vCIO means virtual Chief Information Officer, a planning role that helps a business think through technology priorities, budgets, and risk.

How to score yourself

If you answered Yes to most items, that is a good sign. It usually means you have a workable foundation. That does not make your business “fully secure.” No honest provider promises an unhackable network or zero downtime. It means you likely have the basics in place and can improve from there.

If you answered No or Not sure to several items, do not panic. That is common, especially in smaller businesses where technology has grown informally over time. Start with the basics that usually matter most first: MFA, patching, backups, removing old access, device protection, and basic staff training.

If almost everything is No or Not sure, the next step is not to buy every tool at once. It is to get a clear, prioritized plan. A good independent managed IT provider can help you sort urgent fixes from longer-term improvements.

What to do with your answers

Turn your results into a short action list with three groups: fix now, fix soon, and review later. “Fix now” usually includes MFA, software updates, backup checks, removing old accounts, and making sure business devices have current protection.

For each No or Not sure, ask a plain question. Who owns this? How often is it done? Is it written down? How do we know it worked? Those four questions will reveal whether a process is real or only assumed.

If you want help understanding your options, NodeBridge IT can connect you with an independent managed IT services provider. We are a free matching service. We do not manage systems, monitor your network, or access your accounts. You can also read more plain-language guides and compare common managed IT services.

- Fix now: MFA, patching, backups, old account cleanup, device protection
- Fix soon: staff training, device and software inventory, remote work rules, vendor list

- Review later: planning, documentation, service agreements, long-term security improvements

Quick answers

What is a good score on this checklist?

There is no universal passing score. If you have solid answers for the main basics, especially MFA, backups, updates, and access control, you likely have a better starting point than many small businesses. If you have many No or Not sure answers, that is a sign to prioritize improvements.

Can this checklist replace a real security review?

No. This is a plain-language self-check, not a technical assessment or compliance review. It helps you see where to ask better questions and where an independent provider may need to look more closely.

We are a very small business. Do we really need all of this?

Most very small businesses still need the basics. Shared passwords, missing updates, and weak backups can create expensive problems even in a small office. The exact setup should fit your size, data, and industry.

What if I do not know how to answer some of these?

Mark Not sure. That is still useful. It often means the process is unclear, not documented, or depends on one person or one vendor.

Can NodeBridge IT tell us which security tools to buy?

We provide general educational information and free matching. We do not sell or manage security tools, and we do not access your systems. If you want outside help, we can help you find an independent managed IT provider to talk through options.

Do we need to share passwords or technical details to get matched?

No. Never send us passwords, network credentials, or system access. We only collect basic business and contact details so we can help connect you with a provider.

NodeBridge IT is a free matching service, not a managed IT provider or security firm. The information here is general and educational. No one can guarantee uptime, security, or recovery. Confirm scope, response times, and price in writing with any provider before you sign. Find more at nodebridgeit.pages.dev or contact hello@nodebridgeit.com.