Free resource kit for small business owners

The Small Business IT Kit

Find hidden risks. Cut IT waste. Use AI safely.

Inside this kit

Scorecard	The 15-Minute Business Technology Health Check
Checklist	The Small Business Cybersecurity Checklist: 12 Things to Check Today
Checklist	The IT Cost-Cutting Checklist: 10 Ways to Stop Wasting Money on Technology
Guide	The SMB Guide to Practical AI: 10 Ways to Save Time Without Putting Your Business Data at Risk

How to use it: Start with the 15-minute health check to see where you stand. Then use the cybersecurity and cost checklists to close the gaps it finds, and the AI guide when you're ready to save time safely.

About Beanstalk Computing
Beanstalk.it provides managed IT services for San Diego businesses, combining responsive support with modern AI solutions. Plans are flat-rate and tailored to each business, with 24/7 monitoring, cybersecurity protection and cloud solutions included where you need them.

Self-assessment scorecard

The 15-Minute Business Technology Health Check

Fifteen quick questions to see where your technology is helping your business, and where it's putting it at risk.

Technology problems rarely announce themselves. A backup that quietly stopped running, a former employee who can still log in, a laptop that hasn't updated in a year: these are the gaps that turn a normal Tuesday into a crisis. This health check takes about 15 minutes and shows you where to look first.

How it works: Answer each question with the option that best describes your business today and check the box. Add up the points in each section, then total your score on the last page. Be honest; the goal is to find gaps, not to pass.

Backup and recovery

Section score: _____ / 6

1. How is your business data backed up?

- ☐ No regular backup, or not sure — 0 pts
- ☐ Some data, manually or to one location — 1 pt
- ☐ Automatic backups to a separate offsite or cloud location — 2 pts

2. When did you last test restoring files from a backup?

- ☐ Never, or not sure — 0 pts
- ☐ More than a year ago — 1 pt
- ☐ Within the last six months — 2 pts

3. If your main computer or server failed today, how long until you're working again?

- ☐ Not sure, or several days — 0 pts
- ☐ About a day — 1 pt
- ☐ A few hours, and we have a written plan — 2 pts

Security basics

Section score: ____ / 6

4. Is multi-factor authentication (MFA) turned on for company email?

- [ ] No, or not sure — 0 pts
- [ ] For some people — 1 pt
- [ ] For everyone, including admin accounts — 2 pts

5. How does your team store passwords?

- [ ] Reused, written down or shared — 0 pts
- [ ] Mixed habits across the team — 1 pt
- [ ] A company password manager with unique passwords — 2 pts

6. Has your team had security awareness or phishing training?

- [ ] Never — 0 pts
- [ ] Once, a while ago — 1 pt
- [ ] Within the last year, with regular refreshers — 2 pts

Devices and updates

Section score: ____ / 6

7. How are operating system and software updates handled?

- [ ] When someone remembers — 0 pts
- [ ] Automatic on some devices — 1 pt
- [ ] Automatic and monitored on every device — 2 pts

8. Do all your computers run a current, supported operating system?

- [ ] Some don't, or not sure — 0 pts
- [ ] Most do — 1 pt
- [ ] All do, and we have a replacement schedule — 2 pts

9. Is every device protected by security software that someone monitors?

- [ ] Free antivirus or none — 0 pts
- [ ] Paid antivirus, but nobody watches the alerts — 1 pt
- [ ] Endpoint protection monitored by our IT provider — 2 pts

Support and downtime

Section score: ____ / 6

10. When something breaks, who fixes it?

- [ ] Whoever on staff is good with computers — 0 pts
- [ ] We call someone after it breaks — 1 pt
- [ ] Dedicated IT support with agreed response times — 2 pts

11. How often do technology problems interrupt work?

- [ ] Weekly or more — 0 pts
- [ ] A few times a month — 1 pt
- [ ] Rarely — 2 pts

12. Are your systems monitored so problems are caught before they stop work?

- [ ] No — 0 pts
- [ ] Partly — 1 pt
- [ ] Yes, around the clock — 2 pts

Access, costs and planning

Section score: ____ / 6

13. When an employee leaves, how fast is their access removed?

- [ ] Not always removed — 0 pts
- [ ] Within a week or so — 1 pt
- [ ] Same day, using a checklist — 2 pts

14. Do you know what you spend on technology each year?

- [ ] No idea — 0 pts
- [ ] A rough idea — 1 pt
- [ ] Yes, with a budget and predictable monthly costs — 2 pts

15. Do you have a technology plan for the next 12 months?

- [ ] No — 0 pts
- [ ] Informal ideas only — 1 pt
- [ ] A written plan, reviewed with an IT advisor — 2 pts

Your results

Section	Your score
Backup and recovery	____ / 6
Security basics	____ / 6
Devices and updates	____ / 6
Support and downtime	____ / 6
Access, costs and planning	____ / 6
Total	**____ / 30**

What your score means

0 to 12	**At risk** Your business is exposed to downtime and data loss that could be avoided. Start this week with backups and multi-factor authentication.
13 to 22	**Getting by** Some basics are in place, but real gaps remain. Fix your lowest-scoring section first, then work up.
23 to 30	**In good shape** Your foundation is solid. Keep it that way with regular restore tests, access reviews and a written plan.

Where to focus first

Look at your lowest section score. Any section under 3 points is a priority. A zero in **Backup and recovery** or **Security basics** is the most urgent of all, because those gaps can stop your business entirely, not just slow it down.

Want a second opinion on your score?

Beanstalk Computing can walk through your answers with you and build a plan that fits your size and budget, with flat-rate monthly pricing and 24/7 monitoring. Visit beanstalkit.com.

Security checklist

The Small Business Cybersecurity Checklist: 12 Things to Check Today

The basics that stop the most common attacks, and how to confirm each one is really in place.

Most attacks on small businesses don't start with sophisticated hacking. They start with a stolen password, a missed update or a convincing email. These 12 checks cover the basics that stop the most common attacks. Work through them with whoever manages your IT; most take only minutes to verify.

- [ ] **1. Multi-factor authentication is on for email and every admin account**
  Why it matters: A stolen password is the most common way attackers get in. MFA stops most of those logins cold.
  How to check: In your Microsoft 365 or Google Workspace admin center, confirm MFA is required for every user, not just offered.

- [ ] **2. Updates install automatically on every computer and phone**
  Why it matters: Attackers target known flaws that already have a fix. Unpatched devices are open doors.
  How to check: Spot-check three computers: are Windows or macOS updates current, and is the operating system still supported?

- [ ] **3. Backups run automatically, live offsite, and a restore has been tested**
  Why it matters: Ransomware and hardware failure are survivable when you can restore. A backup you've never tested is a guess.
  How to check: Ask for the date of the last successful backup and the last test restore. Both should be recent.

- [ ] **4. Every device has endpoint protection that someone watches**
  Why it matters: Modern threats slip past basic antivirus. Alerts only help if a person responds to them.
  How to check: Confirm which tool protects each device and who receives and acts on its alerts, including nights and weekends.

- [ ] **5. Former employees and vendors no longer have access**
  Why it matters: Old accounts are easy to forget and easy to misuse.
  How to check: Compare your list of active accounts against your current staff list. Disable anything that doesn't match.

- [ ] **6. The team uses a password manager, with no shared or reused passwords**
  Why it matters: One reused password can unlock email, banking and client systems at once.
  How to check: Ask: do we have a company password manager, and is everyone actually using it?

- [ ] **7. Staff don't use administrator accounts for everyday work**
  Why it matters: If an everyday account is compromised, admin rights let malware install itself and spread.
  How to check: Check whether regular users can install software on their own. If they can, admin rights are too broad.

- [ ] **8. Email security is configured, including SPF, DKIM and DMARC**
  Why it matters: These settings make it harder for criminals to send email that looks like it came from your domain.
  How to check: Ask your IT provider to confirm all three records are set up, and that spam and attachment filtering is on.

- [ ] **9. Your firewall and Wi-Fi are updated and locked down**
  Why it matters: Default passwords and outdated router firmware are easy targets.
  How to check: Confirm default admin passwords were changed, firmware is current, and guest Wi-Fi is separate from business systems.

- [ ] **10. Staff know how to spot phishing, and payment changes are verified by phone**
  Why it matters: Many costly attacks rely on a convincing email, not on hacking. A simple call-back rule stops payment fraud.
  How to check: Confirm training happened within the last year, and that bank detail changes are always verified with a known number.

- [ ] **11. Laptops and phones are encrypted and can be wiped remotely**
  Why it matters: A lost device shouldn't turn into a data breach.
  How to check: Check that disk encryption (BitLocker or FileVault) is on and that company phones are enrolled in device management.

- [ ] **12. You have a written plan for a security incident**
  Why it matters: In the first hour of an attack, decisions made in panic cost the most.
  How to check: Make sure it's written down and shared: who to call, what to disconnect, and how to reach your team if email is down.

Count your checks

11 to 12 checked	A strong foundation. Re-check every quarter so it stays that way.
7 to 10 checked	Real gaps remain. Fix items 1 to 4 first if any are unchecked; they stop the most attacks.
0 to 6 checked	Your business is at high risk. Get help this month, starting with MFA, backups and updates.

Handle regulated data?

Healthcare practices, law firms and financial businesses may have additional requirements, such as HIPAA. This checklist covers the basics, not compliance. Ask your IT provider to map these checks to your specific obligations.

Not sure how to check some of these?

Beanstalk Computing provides cybersecurity protection for San Diego businesses, including firewall and endpoint protection, security monitoring, backup and disaster recovery, and employee security training. Visit beanstalkit.com.

Cost checklist

The IT Cost-Cutting Checklist: 10 Ways to Stop Wasting Money on Technology

Find the forgotten subscriptions, unused licenses and surprise bills that drain your budget.

Most small businesses don't overspend on technology through one big mistake. They overspend through dozens of small ones: forgotten subscriptions, unused licenses and surprise repair bills. This checklist helps you find and stop that waste without cutting what your team actually needs.

- [ ] **1. Cancel software subscriptions nobody uses**

  Where the money goes: Subscriptions pile up as teams try new tools, and many keep billing long after people stop using them.

  What to do: Pull 12 months of card and invoice charges, list every software subscription, and ask each owner if it's still used.

- [ ] **2. Remove licenses for people who have left**

  Where the money goes: Paying for a departed employee's email and software licenses is one of the most common silent costs.

  What to do: Compare paid licenses in Microsoft 365 or Google Workspace against your current staff list.

- [ ] **3. Put each person on the right license tier**

  Where the money goes: Not everyone needs the premium plan. Others may be paying separately for features their plan already includes.

  What to do: Review who uses which features, then move people up or down a tier to match.

- [ ] **4. Consolidate tools that do the same job**

  Where the money goes: Two file-sharing services, three chat apps and two video tools mean double the cost and scattered data.

  What to do: List tools by job (files, chat, video, e-signature). Pick one per job and retire the rest.

- [ ] **5. Review phone and internet bills**

  Where the money goes: Unused phone lines, outdated plans and old equipment rentals often stay on the bill for years.

  What to do: Match every line and service on the bill to a current person or location. Ask your provider about current plans.

- [ ] **6. Replace hardware on a schedule, not in emergencies**

  Where the money goes: Emergency purchases cost more, and aging machines waste staff time every day before they finally fail.

  What to do: Track the age of every computer. Budget to replace the oldest ones each year instead of waiting for failures.

- [ ] **7. Swap surprise repair bills for predictable support**

  Where the money goes: Break-fix support makes costs unpredictable and gives no one a reason to prevent problems.

  What to do: Add up last year's emergency IT invoices and compare them against a flat-rate managed support plan.

- [ ] **8. Know what downtime really costs you**

  Where the money goes: An hour of lost work is a cost even when no invoice shows it. Prevention is usually cheaper than recovery.

  What to do: Use the worksheet on the next page to estimate the cost of one hour of downtime for your business.

- [ ] **9. Right-size cloud storage and services**

  Where the money goes: Cloud costs grow quietly: old backups, idle servers and storage nobody cleans up.

  What to do: Ask for a list of every cloud service and its monthly cost. Delete or downsize anything idle.

- [ ] **10. Automate repetitive work**

  Where the money goes: Hours spent re-typing data, chasing approvals and copying files between systems add up fast.

  What to do: Ask your team which task they repeat most each week. Start there; many can be automated with tools you already own.

Worksheet: what does an hour of downtime cost you?

Fill this in once. It puts a real number on every outage, slow computer and failed backup.

Number of people who can't work	_____
Average hourly cost per person (pay plus benefits)	$ _____
Labor cost per hour (multiply the two lines above)	$ _____
Revenue lost per hour (sales or billable work that stops)	$ _____
Cost of one hour of downtime	**$ _____**

Illustrative example only: 10 people at $40 an hour is $400 in labor, plus $500 in lost sales, for a total of about $900 for every hour systems are down. Your numbers will differ.

Savings tracker

List what you found as you work through the checklist.

Item	Monthly cost today	Action	Monthly savings
	$		$
	$		$
	$		$
	$		$
	$		$
	$		$
Total			**$**

Want predictable IT costs?

Beanstalk Computing manages IT for a flat monthly fee, with no extra charge when a server fails or the network has issues. Plans are tailored to your business size, goals and budget. Visit beanstalkit.com.

Practical guide

The SMB Guide to Practical AI: 10 Ways to Save Time Without Putting Your Business Data at Risk

Where AI saves real hours for a small business, and the simple guardrails that keep your data where it belongs.

AI tools can take hours of routine work off your team's plate every week. The catch is that whatever employees type or paste into an AI tool may leave your control. This guide covers 10 practical ways to save time, with the guardrail to put in place for each one.

Five rules before you start

- [ ] **Use business accounts, not personal ones.** Business plans of AI tools give you admin control and clearer terms on how your data is handled.
- [ ] **Know what never goes into a free tool.** Client records, health or legal information, financial details, passwords and anything under NDA.
- [ ] **Check the data settings.** Find out whether the tool keeps your prompts and whether they're used to train its models, then set it accordingly.
- [ ] **Clean up file permissions first.** AI assistants built into email and file systems can surface anything a user has access to, including files they shouldn't.
- [ ] **Keep a person in the loop.** AI drafts and summarizes; people check facts, numbers and anything that goes to a client.

10 ways to save time

1. Draft and reply to email faster

Time saver: Turn bullet points into a clear reply, or soften the tone of a tricky message.
Data guardrail: Remove client names and account details unless you're using an approved business tool.

2. Summarize meetings and calls

Time saver: Get action items and decisions from a recorded meeting in minutes instead of rewriting notes.

Data guardrail: Tell attendees when meetings are recorded, and confirm where recordings and transcripts are stored.

3. Write first drafts of proposals and marketing

Time saver: Get past the blank page on proposals, web copy, job posts and social content.

Data guardrail: Fact-check every claim, price and promise before anything is published or sent.

4. Find answers in your own documents

Time saver: Ask questions of your policies, price lists and past proposals instead of digging through folders.

Data guardrail: Only connect AI to systems where file permissions are cleaned up and set correctly.

5. Answer common customer questions

Time saver: Draft consistent answers to frequent questions about hours, services and next steps.

Data guardrail: Have a person review responses before customers see them, and never let AI make commitments on your behalf.

6. Summarize long documents

Time saver: Get the key points of a long contract, report or vendor agreement before you read the full text.

Data guardrail: A summary is not legal advice. Have a qualified person review anything you plan to sign.

7. Work with spreadsheets

Time saver: Get help writing formulas, cleaning messy data and spotting trends in a report.

Data guardrail: Use de-identified or sample data unless the tool is approved for financial information.

8. Automate repetitive workflows

Time saver: Route intake forms, sort requests and fill in routine fields automatically.

Data guardrail: Start with low-risk tasks and check the results before trusting the automation with anything important.

9. Create training guides and SOPs

Time saver: Turn a recorded walkthrough or rough notes into a step-by-step guide for new hires.

Data guardrail: Have the person who does the task review the guide for accuracy before it's shared.

10. Research and brainstorm

Time saver: Explore ideas, compare options and prepare questions before meeting a vendor or client.

Data guardrail: AI can state wrong information confidently. Verify facts with original sources.

Write a one-page AI policy

You don't need a legal document to start. A single page that answers these questions keeps your team moving fast and your data in the right place:

- [ ] Which AI tools are approved, and which accounts staff should use
- [ ] What information can and can't be entered into each tool
- [ ] Who reviews AI-assisted work before it reaches a client
- [ ] How to report a mistake, such as sensitive data pasted into the wrong tool
- [ ] Who owns the policy and when it gets reviewed

Healthcare and legal practices: before using any AI tool with patient or client information, confirm the vendor will sign the agreements your regulations require, such as a HIPAA business associate agreement.

Want help putting AI to work safely?

Beanstalk Computing combines managed IT with modern AI solutions that help businesses work smarter, automate processes and protect their data. Visit beanstalkit.com.