ADNET® TECHNOLOGIES
A New Charter Technologies Company

COMPLETE RESOURCE KIT

The Business Technology Kit

This kit contains all four tools in one file.

TOOL 1 — Business Technology Health Check
TOOL 2 — Cybersecurity Checklist
TOOL 3 — Technology Cost-Cutting Checklist
TOOL 4 — Practical AI Guide

Developed by Xplifi, sponsored by ADNET Technologies.
General guidance only. Not legal, compliance, financial or professional security advice.

What's in this kit

Four practical tools for reviewing your business technology. Each tool can also be downloaded on its own.

TOOL 1
Business Technology Health Check
The 15-Minute Business Technology Health Check
page 3

TOOL 2
Cybersecurity Checklist
The Small Business Cybersecurity Checklist: 12 Things to Check Today
page 7

TOOL 3
Technology Cost-Cutting Checklist
The IT Cost-Cutting Checklist: 10 Ways to Stop Wasting Money on Technology
page 12

TOOL 4
Practical AI Guide
The SMB Guide to Practical AI: 10 Ways to Save Time Without Putting Your Business Data at Risk
page 16

Developed by Xplifi, sponsored by ADNET Technologies. This kit offers general guidance and is not legal, compliance, financial or professional security advice.

ADNET® TECHNOLOGIES
A New Charter Technologies Company

TOOL 1

Business Technology Health Check

The 15-Minute Business Technology Health Check

Is your business technology helping you grow—or holding you back?

Inside this tool

- 18 yes/no questions across seven areas
- A results guide: Good, Needs Attention or At Risk
- Three recommended next steps

Developed by Xplifi, sponsored by ADNET Technologies.
General guidance only. Not legal, compliance, financial or professional security advice.

How to use this check

This check doesn't assume you've had a security incident or that you're trying to cut costs. It gives you a quick, plain-language view of whether your technology is reliable and where it needs attention.

1. Set aside about 15 minutes and answer each question for your organization as it is today.
2. Tick **Yes** or **No**. If you're not sure, tick No — uncertainty is a sign the item needs a closer look.
3. Count your Yes answers and use the results guide at the end.

Device and software maintenance

1	Is every computer running an operating system version that still receives security updates from its maker?	☐ Yes	☐ No
2	Are software and operating system updates installed on a regular schedule, not only when someone remembers?	☐ Yes	☐ No
3	Do you have a current list of your organization's computers and devices, and who uses each one?	☐ Yes	☐ No

Network reliability and performance

4	Is your internet connection reliable enough that outages rarely interrupt work?	☐ Yes	☐ No
5	Does your Wi-Fi cover the spaces where people work without frequent drops or slowdowns?	☐ Yes	☐ No
6	Is your network equipment (router, firewall, switches) still supported and receiving updates?	☐ Yes	☐ No

Data backup and recovery

7	Is important business data backed up automatically?	☐ Yes	☐ No
8	Is at least one backup copy kept separately from your main systems, for example off-site or in the cloud?	☐ Yes	☐ No
9	Have you restored files from a backup in the past year to confirm the backup actually works?	☐ Yes	☐ No

Cybersecurity basics

10 Is multi-factor authentication turned on for email and other key business accounts? ☐ Yes ☐ No

11 Is security software installed and active on every computer? ☐ Yes ☐ No

12 Have employees been shown how to recognize a suspicious email or link? ☐ Yes ☐ No

Employee access and account management

13 When someone leaves, are their accounts and access removed promptly? ☐ Yes ☐ No

14 Do people have access only to the systems and data they need for their role? ☐ Yes ☐ No

Technology support responsiveness

15 Do employees know exactly who to contact when something stops working? ☐ Yes ☐ No

16 Are support requests usually resolved quickly enough that work isn't held up? ☐ Yes ☐ No

Recurring technology issues

17 Are you free of the same problems (slow computers, printer failures, connection drops) coming back again and again? ☐ Yes ☐ No

18 Is there a plan to replace aging equipment before it fails? ☐ Yes ☐ No

Notes and follow-ups

Your results

Count your Yes answers out of 18 and write the total here.

My Yes total: _____ / 18

Good 15–18 Yes answers	Your technology foundations look solid. Keep them that way by repeating this check at least once a year and after any big change, such as a move or new system.
Needs Attention 10–14 Yes answers	The basics are partly in place, but some gaps could cause disruption. Work through your No answers, starting with data backup and cybersecurity basics.
At Risk 0–9 Yes answers	Several gaps could affect day-to-day work or leave business data poorly protected. Treat your No answers as a priority list and address the backup and security items first.

Whatever your total, any No in Data backup and recovery or Cybersecurity basics deserves attention.

Three recommended next steps

1. **List every No answer** and note who in your organization is responsible for it.
2. **Fix the quick wins first.** Some items, such as turning on multi-factor authentication or confirming a backup works, can often be resolved in a day.
3. **Schedule a follow-up review** in three to six months. For items you can't resolve internally, get a second opinion from a qualified technology provider.

About ADNET Technologies

ADNET Technologies provides Managed IT, Cybersecurity, Cloud and AI + automation services to Connecticut and Capital Region organizations. Its fully managed service, TotalCare, is described as including unlimited remote support via chat, phone or email, 24/7 IT support options, onsite support as needed and proactive system care. ADNET also describes firewall monitoring and management (Foundations Firewall).

thinkadnet.com

Company details as reported by ADNET Technologies.

ADNET® TECHNOLOGIES
A New Charter Technologies Company

TOOL 2

Cybersecurity Checklist

The Small Business Cybersecurity Checklist: 12 Things to Check Today

Could your business be exposed to a cyberattack?

Inside this tool

- 12 checks you can complete yourself
- Why each item matters
- What to do if something is missing

Developed by Xplifi, sponsored by ADNET Technologies.
General guidance only. Not legal, compliance, financial or professional security advice.

How to use this checklist

Cybersecurity can feel complex, especially without an internal technology team. This checklist breaks it into 12 practical checks you can complete yourself. Tick each item that is already in place. For anything you can't tick, the "If it's missing" note suggests a practical first step.

No checklist can guarantee protection. These checks help reduce common, everyday risks.

☐ **Email security and phishing protection** — 01 of 12

Your email service filters spam, malicious attachments and suspicious links before they reach inboxes.

Why it matters
Email is one of the most common ways attackers try to reach a business and its people.

If it's missing
Review the security and filtering settings in your email platform, or ask your email provider or IT support what protection is turned on.

☐ **Strong, unique passwords** — 02 of 12

Every account uses its own strong password, ideally stored in a business password manager.

Why it matters
When one password is reused, a single leak can open several accounts.

If it's missing
Adopt a password manager and replace reused passwords, starting with email, banking and administrator accounts.

☐ **Multi-factor authentication (MFA)** — 03 of 12

MFA is turned on for email, remote access, banking and administrator accounts.

Why it matters
MFA adds a second check, so a stolen password alone isn't enough to sign in.

If it's missing
Turn on MFA for email and administrator accounts first, then extend it to your other business systems.

☐ **Employee access and account permissions** — 04 of 12

People can reach only the data and systems their role requires, and few accounts have administrator rights.

Why it matters
Limiting access limits how far a problem can spread from one compromised account.

If it's missing
Review who can access what, remove permissions that aren't needed and keep administrator rights to a small group.

Accounts for people who have left

05 of 12

Former employees' and contractors' accounts are disabled on their last day.

Why it matters
Unused accounts are easy to overlook and can be misused long after someone has gone.

If it's missing
Create a simple offboarding checklist and compare your active accounts with your current staff list.

Computer and device protection

06 of 12

Every laptop, desktop and mobile device has security software, a screen lock and encryption where available.

Why it matters
A lost or unprotected device can expose the business data stored on it.

If it's missing
Turn on built-in encryption and screen locks, and confirm security software is installed and current on each device.

Network and Wi-Fi security

07 of 12

Wi-Fi uses strong encryption and a strong password, guests use a separate network and default router passwords have been changed.

Why it matters
A poorly secured network can give outsiders a path to your devices and data.

If it's missing
Change default passwords, set up a separate guest network and confirm your router or firewall software is up to date.

Data backups and recovery

08 of 12

Important data is backed up automatically, a copy is kept separately from your main systems, and restores are tested.

Why it matters
Backups are how you recover from hardware failure, human error or ransomware.

If it's missing
Identify your critical data, set up automatic backups with an off-site or cloud copy, then test a restore.

Software updates and patching

09 of 12

Operating systems, applications and network devices receive updates promptly.

Why it matters
Updates close known security weaknesses that attackers look for.

If it's missing
Turn on automatic updates where possible and set a regular schedule for anything that needs manual updating.

Employee cybersecurity awareness

10 of 12

Staff know how to spot phishing, how to handle sensitive information and who to tell when something looks wrong.

Why it matters
People are part of your defense. A quick report can stop a problem from spreading.

If it's missing
Run a short awareness session and share one clear contact for "if in doubt, report it."

Third-party access

11 of 12

You know which vendors and contractors can reach your systems or data, and their access is limited and reviewed.

Why it matters
Outside access is easy to forget once a project or contract ends.

If it's missing
List every third party with access, remove what's no longer needed and require MFA for the rest.

Incident response preparation

12 of 12

You have a written plan for what to do if you suspect a security incident, including who to call.

Why it matters
Knowing the first steps in advance saves time and reduces confusion under pressure.

If it's missing
Write a one-page plan covering who to contact, how to disconnect affected devices and how to reach your backups.

Your checklist summary

Count the items you ticked and write the total here.

Items in place: _____ / 12

Where to start if items are missing

1. **Protect your accounts first.** Multi-factor authentication and unique passwords (items 2 and 3) are often quick to put in place and cover your most important logins.
2. **Make sure you can recover.** Confirm that backups run automatically and that a restore has been tested (item 8).
3. **Close the known gaps.** Turn on automatic updates (item 9) and remove access for people and vendors who no longer need it (items 5 and 11).
4. **Prepare your people.** A short awareness session and a one-page incident plan (items 10 and 12) help everyone respond calmly if something goes wrong.

Revisit this checklist regularly, and whenever you add new staff, systems or vendors. If an item is outside your team's experience, a qualified technology provider can help you put it in place.

About ADNET Technologies

ADNET Technologies provides Managed IT, Cybersecurity, Cloud and AI + automation services to Connecticut and Capital Region organizations. Its fully managed service, TotalCare, is described as including unlimited remote support via chat, phone or email, 24/7 IT support options, onsite support as needed and proactive system care. ADNET also describes firewall monitoring and management (Foundations Firewall).

thinkadnet.com

Company details as reported by ADNET Technologies.

ADNET® TECHNOLOGIES
A New Charter Technologies Company

TOOL 3

Technology Cost-Cutting Checklist

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

Are you paying for technology your business does not need or use?

Inside this tool

- 10 areas to review for wasted spend
- What to look for in each area
- A monthly technology expense worksheet

Developed by Xplifi, sponsored by ADNET Technologies.
General guidance only. Not legal, compliance, financial or professional security advice.

How to use this checklist

Cost control is a familiar business priority, and technology spending is easy to lose track of. Work through the ten areas below and tick each one once you've reviewed it. Then use the monthly expense worksheet to list what you pay for and decide what to look at first.

Treat each item as an opportunity to investigate. Actual savings depend on your contracts, your usage and what your business needs.

☐ Identify unused software subscriptions

01 of 10

What to look for
Subscriptions nobody has signed in to recently, and free trials that quietly became paid plans.

Opportunity to investigate
Review card and invoice statements for recurring software charges and confirm each one is still used.

☐ Remove duplicate tools and services

02 of 10

What to look for
Two or more tools doing the same job, such as separate file-sharing or video-meeting services.

Opportunity to investigate
Choose one tool per job and plan the move away from the others before their next renewal.

☐ Review software licenses and user accounts

03 of 10

What to look for
Licenses still assigned to people who have left, or plan levels higher than people need.

Opportunity to investigate
Match license counts to your current staff and check whether each person needs the plan level they have.

☐ Evaluate hardware replacement needs

04 of 10

What to look for
Older equipment that is slow, out of warranty or regularly costing staff time.

Opportunity to investigate
Compare the cost of repairs and lost time with planned replacement, rather than buying in an emergency.

☐ Review recurring technology expenses

05 of 10

What to look for
Phone lines, internet service, hosting, maintenance contracts and other charges that renew automatically.

Opportunity to investigate
List every recurring charge with its renewal date and contract term so nothing renews by default.

☐ Identify costly recurring technical problems

06 of 10

What to look for
The same issues coming back and taking staff time each time they happen.

Opportunity to investigate
Track recurring problems for a month. Fixing the cause may cost less than repeated workarounds.

☐ Check maintenance and support arrangements

07 of 10

What to look for
Support on equipment you no longer use, overlapping contracts or frequent paid emergency call-outs.

Opportunity to investigate
Compare what each agreement covers with what you actually use and need.

☐ Reduce downtime-related costs

08 of 10

What to look for
Time lost when systems, internet or key applications are unavailable.

Opportunity to investigate
Note recent outages and how long they lasted, then focus on the causes that keep repeating.

☐ Review cloud storage and service usage

09 of 10

What to look for
Storage that keeps growing, old files no one needs and cloud services that are no longer in use.

Opportunity to investigate
Archive or delete what isn't needed and check that each service is on the right plan.

☐ Plan technology spending more effectively

10 of 10

What to look for
Purchases made only when something breaks, with no budget or replacement schedule.

Opportunity to investigate
Create a simple annual technology budget and a replacement schedule for key equipment.

Notes and follow-ups

Monthly technology expense worksheet

List each technology expense as a monthly amount (divide annual charges by 12). Mark whether it's still needed, note any possible saving to investigate and give it a priority: H (high), M (medium) or L (low).

Expense or service	Provider	Monthly cost	Users / seats	Still needed? Y / N	Possible saving to investigate	Priority
Software subscriptions		$			$	
Email and productivity		$			$	
Phone and internet		$			$	
Cloud storage and hosting		$			$	
Security tools		$			$	
Hardware maintenance		$			$	
IT support and services		$			$	
Printing and copiers		$			$	
		$			$	
		$			$	
		$			$	
		$			$	
Monthly total		**$**			**$**	

Tip: Start with the high-priority rows that are no longer needed or duplicate another tool. Check notice periods and renewal dates before cancelling anything.

About ADNET Technologies

ADNET Technologies provides Managed IT, Cybersecurity, Cloud and AI + automation services to Connecticut and Capital Region organizations. Its fully managed service, TotalCare, is described as including unlimited remote support via chat, phone or email, 24/7 IT support options, onsite support as needed and proactive system care. ADNET also describes firewall monitoring and management (Foundations Firewall).

thinkadnet.com

Company details as reported by ADNET Technologies.

ADNET® TECHNOLOGIES
A New Charter Technologies Company

TOOL 4

Practical AI Guide

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

Are you missing opportunities to save time and improve productivity with AI in your business?

Inside this tool

- 10 practical ways to use AI
- What never to enter into public AI tools
- Basic usage guidelines and an AI Readiness Checklist

Developed by Xplifi, sponsored by ADNET Technologies.
General guidance only. Not legal, compliance, financial or professional security advice.

Getting started with AI, safely

AI tools are becoming part of everyday business software, but many owners aren't sure where to start, which tasks suit AI or how to use it responsibly. These ten practical uses show where AI can save time, with a data-safety note for each one.

1 Draft and improve business communications

How it saves time
Use AI to produce a first draft of emails, letters and announcements, or to tighten wording and adjust tone.

Keep data safe
Leave out client names and confidential details, and have a person check every draft before it is sent.

2 Summarize documents, reports and meeting notes

How it saves time
Ask for a short summary, key points or action items from long documents and notes.

Keep data safe
Only use documents you're allowed to share with the tool, and check summaries against the original.

3 Automate repetitive administrative tasks

How it saves time
Speed up routine work such as formatting, first-pass data entry, templates and checklists.

Keep data safe
Start with low-risk tasks and keep a person responsible for checking the output.

4 Assist with customer service responses

How it saves time
Draft replies to common questions so staff can respond faster and more consistently.

Keep data safe
Don't paste customer personal or account details into public tools; review every reply before it goes out.

5 Organize information and internal knowledge

How it saves time
Turn scattered notes into clear procedures, FAQs and how-to guides your team can find and follow.

Keep data safe
Keep internal documents in approved tools and limit access to the people who need them.

6 Support marketing content and brainstorming

How it saves time
Generate ideas for posts, headlines and campaign themes, then refine them in your own voice.

Keep data safe
Fact-check claims, and make sure the final content reflects your business accurately.

7 Analyze business data and identify trends

How it saves time
Ask for help spotting patterns in sales, scheduling or operational data, or explaining a spreadsheet.

Keep data safe
Remove or anonymize sensitive data first, and verify any figures before acting on them.

8 Improve employee productivity

How it saves time
Help staff plan their day, prepare for meetings or learn a new tool more quickly.

Keep data safe
Give employees approved tools and simple guidance, rather than leaving them to find their own.

9 Know what should never go into public AI tools

How it saves time
Be clear about which information stays out of public AI tools, whatever the task.

Keep data safe
See the list on the next page and share it with your team.

10 Establish basic AI usage guidelines for employees

How it saves time
A short written guideline helps everyone use AI consistently and responsibly.

Keep data safe
Cover approved tools, what data is allowed, who reviews output and who to ask with questions.

What should never go into public AI tools

Unless your organization has approved a tool and confirmed how it handles data, keep these out of public AI tools:

- Customer, patient or client personal information
- Passwords, access codes and account numbers
- Financial records, payroll and banking details
- Employee records and HR information
- Contracts, legal documents and confidential agreements
- Unreleased plans, pricing and other trade secrets
- Anything you are legally or contractually required to protect

Basic AI usage guidelines for employees

- **Use approved tools only**, signed in with company accounts and multi-factor authentication where available.
- **Follow the data list above.** If you're unsure whether something can be shared, ask first.
- **Review everything.** AI can be confidently wrong. A person checks facts, numbers and tone before anything is sent or published.
- **Be open about AI use** where it matters to customers, partners or your own internal processes.
- **Know who to ask.** Name one person who answers questions about AI use and keeps these guidelines up to date.

Check the settings and terms of any AI tool your business uses to understand how it stores and uses the information you enter.

About ADNET Technologies

ADNET Technologies provides Managed IT, Cybersecurity, Cloud and AI + automation services to Connecticut and Capital Region organizations. Its fully managed service, TotalCare, is described as including unlimited remote support via chat, phone or email, 24/7 IT support options, onsite support as needed and proactive system care. ADNET also describes firewall monitoring and management (Foundations Firewall). ADNET lists AI + automation among its services; the guidance in this tool is general and educational.

thinkadnet.com

Company details as reported by ADNET Technologies.

AI Readiness Checklist

Tick Yes or No for each statement, then count your Yes answers.

1	We know which AI tools our employees are already using.	☐ Yes	☐ No
2	We have approved specific AI tools for business use.	☐ Yes	☐ No
3	Employees know what information must never be entered into public AI tools.	☐ Yes	☐ No
4	We have a written AI usage guideline, even if it's only one page.	☐ Yes	☐ No
5	A person reviews AI-generated content before it is sent or published.	☐ Yes	☐ No
6	We understand how our AI tools store and use the information we enter.	☐ Yes	☐ No
7	Staff use company accounts with multi-factor authentication for AI tools, not personal accounts.	☐ Yes	☐ No
8	We have identified two or three repetitive tasks where AI could save time.	☐ Yes	☐ No
9	Our business information is organized well enough to find what we'd want AI to help with.	☐ Yes	☐ No
10	Someone is responsible for reviewing AI use and updating our guidelines.	☐ Yes	☐ No

8–10 Yes	Ready to expand. Build on what works and review your guidelines as tools change.
4–7 Yes	Ready to start small. Pick one low-risk task and fill the gaps in your No answers.
0–3 Yes	Build the foundations first: approved tools, a data list and a one-page guideline.

Repeat this checklist every six months as your tools and your team's use of AI change.