BLUEDOBIE DEVELOPING

AI ADVISORY FOR LOCAL SERVICE-BASED SMALL BUSINESSES

What goes in cloud AI. What stays local.

A practical first-pass guide for everyday business AI use.

You do not need to ban AI to protect your business. You also should not paste everything into it. Start with what the information is, who it belongs to, and what could happen if it goes somewhere you did not intend.

DON'T PUT THIS IN AN AI PROMP

Passwords and login credentials
Passwords, recovery codes, and authentication details.

API keys and access tokens
If it proves identity or grants access, keep it out of model context.

Payment-card or banking credentials
AI is not a secret store.

Anything you know you cannot share
A contract, customer agreement, or policy may already answer the question.

STOP AND CHECK FIRST

Customer or employee information
Names, addresses, schedules, account information, or personnel records.

Health, financial, biometric, or children's information
Special rules may apply. Find out what they are before choosing an AI service.

Contracts and confidential information
Including NDA-covered material and information another business trusted you to protect.

Legal disputes or insurance claims
Do not guess. Check first.

Large amounts of internal information
One ordinary detail may be fine. Fifty can tell a different story.

GENERALLY LOWER RISK

Public business information
Website copy, public reviews, and public descriptions.

Marketing ideas and social content
Drafts, captions, campaign ideas, and planning.

De-identified or made-up examples
Remove identifying details before you send.

Abstract problem descriptions
Explain the issue without sharing sensitive data.

Approved internal information
Only after checking that restricted information is not included.

LOOK AT THE PILE

An org chart may not be sensitive. Neither is a vendor name, a renewal month, or a scheduling problem. Put enough ordinary pieces together and someone can learn how your business operates, where it hurts, and what it depends on.

The pieces may be ordinary. The pile may not be.

CLOUD OR LOCAL?

Cloud AI can be a good choice when the information is appropriate for the service and you have reviewed how it handles your data. Local AI can be useful when you want tighter control over sensitive internal context or where information is stored and processed. Neither one is automatically safe.

BEFORE YOU PASTE, ASK:

- ☐ Am I allowed to share it?
- ☐ Does it identify a customer, employee, or another person?
- ☐ Does it contain a credential or secret?
- ☐ Would all of this information together reveal something important about the business?
- ☐ Do I know what this AI service does with what I give it?

Know where your information is going.

BLUEDOBIE DEVELOPING

AI ADVISORY FOR LOCAL SERVICE-BASED SMALL BUSINESSES

Make local AI actually private.

Local gives you control. Security comes from what you do with it.

Running AI on your own computer can give you more control over your information. But local only tells you where the model runs. It does not tell you whether the system around it is secure.

1 THE MACHINE NEEDS A LOCK

- Use a strong device login.
- Turn on full-disk encryption.
- Install security updates.
- Lock the screen when you walk away.

2 THE AI NEEDS A LOCK

- Require authentication.
- Use separate accounts when possible.
- Limit administrative access.
- Being on the same network should not automatically mean trusted.

3 THE SECRETS NEED THEIR OWN LOCK

- Keep passwords, API keys, and tokens out of prompts and AI memory.
- Use a protected password vault or secret store.
- Let tools use credentials without exposing them to the model when possible.

4 THE DATA NEEDS A LOCK

- Do not give the AI automatic access to every file.
- Give it access only to what it needs.
- Keep customer, accounting, and employee records separated.

5 ACTIONS NEED A LOCK

- Reading is one level of access. Changing is another.
- Use human approval for important actions.
- Sending, deleting, publishing, refunds, and financial changes deserve a checkpoint.

6 THE NETWORK NEEDS A LOCK

- Know whether the system actually stays local.
- Check for cloud APIs, telemetry, synced histories, remote storage, and plugins.
- A local interface does not guarantee a local data path.

7 THE BACKUP NEEDS A LOCK, TOO

- Back up important data.
- Protect the backup.
- Keep it separate enough that one failure cannot destroy both copies.
- Make sure you can actually restore it.

8 KNOW WHAT HAPPENED

- Keep useful records of access and important actions.
- Know who used it, what it accessed, what it changed, and whether a human approved it.
- Keep only the logs you need, and protect them.

LOCAL SECURITY IS LAYERS

Device > User > AI > Secrets > Data > Network > Actions > Backup

If one layer fails, the next one still matters.