electricsoftware

Quick guide

Security First AI

Use AI at work without handing it the keys.



1 **The mindset** 2

Rules 1 to 2. Two ideas everything else builds on.

2 **Connections and accounts** 3

Rules 3 to 4. What AI can plug into, and whose account holds your data.

3 **Devices and files** 4

Rules 5 to 6. Where AI runs, and what it can find once it's running.

4 **Your safety net** 5

Rules 7 to 8. Backups AI can't reach, and logs someone reads.

5 **Tricks and scams** 6

Rules 9 to 10. Tricks aimed at your AI, and scams that use AI against your people.

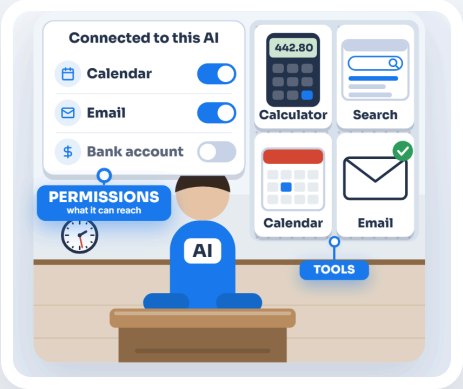
6 **Owning it** 7

Rules 11 to 12. Your responsibility for AI, and the policy and training that go with it.

Chapter 1

The mindset

Two ideas everything else builds on.



1 Give AI the least access it needs

Full guide p. 2

No access by default, read only first, and never more than the person using it.

A simple example. A team assistant is given payroll, HR files and daily reports so it can answer questions. Those files were locked down carefully, but anyone who can use the assistant can now ask it for them. It's the early 2000s spreadsheet problem again. Back then, important numbers sat in one file and nobody controlled who saw it once it was emailed around.

2 Secure AI like a new employee

Full guide p. 3

The same security your people get, plus written instructions: the job, what to deliver, and what it must never do.

A simple example. On day one, a new hire gets their own sign in, access to only the files their job needs, and a manager they answer to. An AI tool your team starts using should get the same, plus written instructions.

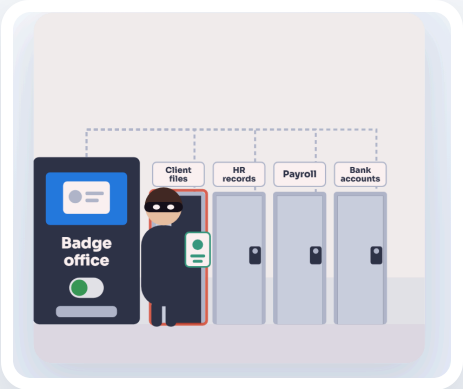
What we do for you

1. We set each AI tool up with only what its job needs, read only wherever the job allows, and connect assistants so each person sees only what they're already allowed to. Anything that changes, sends or deletes waits for a person's approval. On a schedule, we review that access with you and retest what each shared assistant will give out.
2. We run these layers for our clients and add your AI tools to each one. You work with a dedicated engineer who knows your whole setup, and your systems are monitored around the clock.

Chapter 2

Connections and accounts

What AI can plug into, and whose account holds your data.



3 Control what AI connects to

Full guide p. 4

Staff don't connect apps or AI tools on their own. Every connection is approved and gets its own narrow key.

A simple example. In April 2026, an AI coding agent at a software company found a key that had been created for managing custom web domains, but could do anything on the hosting account. It deleted the company's live database, and its backups, in 9 seconds. The hosting company restored the data within an hour (The Register).

4 Keep company data in company accounts

Full guide p. 5

Use business AI accounts with terms you've checked, never personal ones.

A simple example. Two staff members ask the same AI tool to tidy up a customer letter. One uses a company account and the other a free personal one. Only the company account comes with the company's agreement and controls.



What we do for you

3 We switch off one click approvals and go through the apps already approved, removing the ones nobody needs. When staff ask for a new app, we review the request. We also move your tools' keys into a password manager, narrow or replace the ones that open too much, and tell you which vendors only offer keys that open everything.

4 We find what's in use with tools our clients already have, such as web filtering, app control on computers and the Microsoft 365 or Google admin reports, and give you one list. Then we set up the approved tools on company accounts and check their terms. We keep the list up to date as tools come and go.

Chapter 3

Devices and files

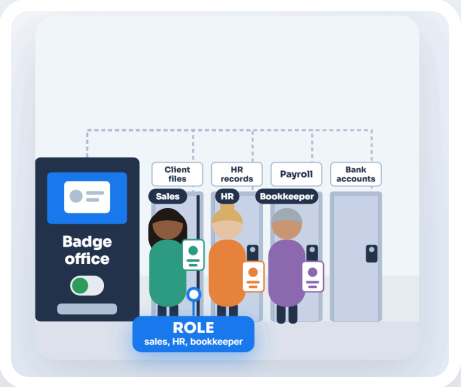
Where AI runs, and what it can find once it's running.

5 Control where AI runs

Full guide p. 5

Only approved AI on company computers, and AI that can operate a computer gets its own isolated machine.

A simple example. An AI that can click, type and open files runs on its own virtual machine. It can reach only the files and tools it has been given for the job, and nothing else on the network.



6 Fix file sharing before AI goes on

Full guide p. 6

AI can open everything your people can, so close old "shared with everyone" folders first.

A simple example. Years ago, someone shared the budget folder with the whole company to get one quick answer, and everyone forgot about it. Today an employee asks the company's AI tool about budgets, and it answers straight from that folder.

What we do for you

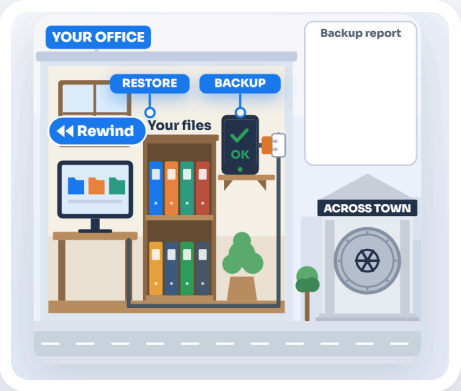
5 On company computers, app control means an AI tool can't run until it's approved, and we can set up an isolated machine for the ones you do approve.

6 We run the sharing reports and fix the worst sites first. Before AI goes on, we fence off the sensitive ones, such as HR and finance.

Chapter 4

Your safety net

Backups AI can’t reach, and logs someone reads.



7 Keep backups AI can’t reach

Full guide p. 6

Limit what AI can delete, and test the restore.

A simple example. In July 2025, an AI coding agent deleted a company’s live database, ignoring an instruction to freeze the code. The instruction had only been typed into the chat, so nothing in the agent’s access enforced it. The data was recovered (The Register).

8 Log and monitor AI activity

Full guide p. 7

Turn on audit logs, and have someone watch AI activity like everything else.

A simple example. A connected app starts downloading every file in the shared drive at 2 a.m. With monitoring, someone gets an alert while it’s happening. Without it, the download could go unnoticed for months.

What we do for you

7 We back up your Microsoft 365 or Google data to a separate service and test restores, so you know how long one takes.

8 We monitor your systems around the clock and add your AI tools’ activity to what we watch.

Chapter 5

Tricks and scams

Tricks aimed at your AI, and scams that use AI against your people.

9 Separate AI roles

Full guide p. 7

Don’t give one AI your data, outside email or web pages, and a way to send things out.

A simple example. In 2025, researchers showed that a single crafted email, never even opened by the person, could make Microsoft’s work assistant leak internal data. Microsoft fixed it, with no sign that anyone had used it (Microsoft’s advisory). Hidden text in a job applicant’s CV could do the same to an AI that screens applications, telling it to approve the candidate.



10 Verify before you act

Full guide p. 8

Check AI work, and confirm money requests on a number you already have.

A simple example. In early 2024, a finance employee at the engineering firm Arup joined a video call with what looked like the CFO and colleagues, and sent about US$25 million in transfers. The CFO and colleagues on the call were deepfakes (CNN).

What we do for you

9 We find which of your AI tools have all three. For those, we limit where they can send things and set up a person’s approval for anything going out.

10 Short security training that repeats, including AI scams, plus browser and app controls on company computers.

Chapter 6

Owning it

Your responsibility for AI, and the policy and training that go with it.

11 Remain responsible

Full guide p. 9

The duty to protect your data stays with you, whichever vendors you use.

A simple example. In 2024, a Canadian tribunal ordered Air Canada to compensate a customer after its website chatbot gave wrong information about a fare (The Register). Air Canada argued the chatbot was responsible for its own actions. The tribunal wrote: "It makes no difference whether the information comes from a static page or a chatbot."

12 Write an AI policy and train staff

Full guide p. 9

Tell staff which AI tools they can use, what they can share, and how to use AI responsibly.

A simple example. A one page policy that names the approved tools, says what must never go into AI, and says who to ask.

What we do for you

11 We keep your list of AI tools and vendors and check their terms. When an insurance or customer questionnaire arrives, we help you answer it with what's actually in place. The duty to protect your data stays with you, and so does the final say.

12 We write your AI use policy with you and keep it current. Your staff get our short, regular training courses on safe AI use and AI scams.

Want more?

Get the full guide. The steps to do each rule yourself, and where the advice comes from.

Take the free AI Check. In about three minutes, see your own gaps and the first fix for each.

Have us do it. A free AI review with our team, then we set it up and keep it running.

Scan or visit

electric.software/ai-security