AI at work, security first

Give AI access to nothing, then grant what it needs, when it needs it.

THE RULES — PAGE IN THE FULL GUIDE

1 **Give AI the least access it needs** p. 2
No access by default, read only first, never more than its user.

2 **Secure AI like a new employee** p. 3
The same security as your staff, plus written instructions.

3 **Control what AI connects to** p. 4
Staff can't connect apps on their own. Every connection is approved.

4 **Keep company data in company accounts** p. 5
Business AI accounts only, never personal ones.

5 **Control where AI runs** p. 5
Approved AI only, and isolate AI that operates a computer.

6 **Fix file sharing before AI goes on** p. 6
AI can open whatever your people can.

7 **Keep backups AI can't reach** p. 6
Limit what AI can delete, and test the restore.

8 **Log and monitor AI activity** p. 7
Audit logs on, and someone watching them.

9 **Separate AI roles** p. 7
Don't give one AI your data, outside content and a way to send things out.

10 **Verify before you act** p. 8
Check AI work, and call back before moving money.

11 **Remain responsible** p. 9
Your duty to protect data stays with you.

12 **Write an AI policy and train staff** p. 9
What staff can use, what they can share, and how.

Do this week

- [ ] Switch staff from personal AI accounts to company ones.
- [ ] Stop staff approving apps themselves, and review the apps already approved.
- [ ] Turn off "Anyone" sharing links before switching AI on.
- [ ] Check who can open your HR and finance files, and what each AI tool can reach.
- [ ] Test a restore, and time it.
- [ ] Agree a call back rule for any request to move money or share records.

Want more?

→ **Get the full guide.** Each rule with the exact settings and a quick check that it's done.

→ **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