A SELF-AUDIT FOR BUSINESS OWNERS AND OFFICE MANAGERS

IT and Data Security Checklist

Thirty plain questions about the things that actually go wrong.

The problems that cost a business real time and money are rarely clever attacks. They are small, ordinary gaps. A backup nobody ever tried to restore. An account still open for someone who left last year. A laptop that never asks for a password.

This is a short self-audit, not an exam. Read each statement and tick the box if it is true for your business today. Where you cannot tick it, or you are not sure, that is your list of things worth a look.

> **How to read it:** there is no score and nothing to hand in. A line you cannot tick is something to fix in the next few months. A line you are not sure about is something to go and check first.

1 Backups

If a file were deleted this afternoon, or a laptop were stolen, how quickly could you be back to normal?

- [ ] Backups run automatically, on a schedule, without anyone having to remember to plug something in.
- [ ] Somebody has tested a restore in the last twelve months, and the file came back working.
- [ ] At least one copy of our data sits somewhere separate from the office, or offline, out of reach of ransomware.
- [ ] Email, accounts and our cloud systems are backed up as well, not just the files on a computer.
- [ ] We know how long we could keep trading without our data, and we are comfortable with that number.

2 Accounts and access

Who can get in, and what happens when someone leaves?

- [ ] We can name everyone with administrator rights, and it is a short list.
- [ ] When someone leaves, their email, files and access are closed down the same day.
- [ ] Multi-factor authentication is switched on for our email, and for Microsoft 365 or Google Workspace.
- [ ] Nobody shares a password, or keeps one in a spreadsheet, a notebook or on a sticky note.
- [ ] We would notice if an account was being used by someone it should not be.

3 Devices

What happens if a laptop is left on a train tonight?

- [ ] Every work laptop and PC is encrypted, so a stolen machine gives up nothing.
- [ ] A lost or stolen device can be locked and wiped remotely, by someone who knows how.
- [ ] Phones and tablets used for work are covered by the same rules as laptops.
- [ ] We have a list of which equipment is with which person, and it gets updated when things change.
- [ ] Nobody uses a personal device for work unless it has been set up and protected properly.

4 Updates and antivirus

Software only protects you when it is current, and someone is watching.

- [ ] Somebody clearly owns Windows, Mac and software updates, and they actually happen.
- [ ] Nothing in the business is still running Windows 10, or another system that is no longer supported.
- [ ] Endpoint protection or antivirus is on every machine, and somebody reviews its warnings rather than ignoring them.
- [ ] Servers, phones and tablets get their updates too, not only the laptops.
- [ ] We would find out within a day if a device had stopped updating or stopped reporting in.

5 Phishing and people

It usually starts with an email that looked perfectly fine.

- [ ] Staff have had some form of security training in the last twelve months.
- [ ] Everyone knows exactly who to tell when an email looks wrong, and they do tell them.
- [ ] Any request to change bank details or pay a new supplier is checked by phone, on a number we already had.
- [ ] There is a written IT policy, about a page long, that staff have actually read.
- [ ] We have talked through what to do if somebody clicks something they should not have.

6 Contracts and continuity

The quiet arrangements that decide how bad a bad day gets.

- [ ] We know when our broadband and telephone contracts end, and how much notice we must give.
- [ ] One named person is responsible for IT, even if that is not their whole job.
- [ ] If the server or main computer died on a Monday morning, we know who we would call and what we would do first.
- [ ] We have cyber insurance, and we know what it expects us to have in place.
- [ ] We could list our key systems and suppliers, and who to contact for each, without looking it up.

What to do next

Go back through the pages. Everything you ticked is solid, so leave it alone and give yourself some credit for it. Everything else is your list, and the useful step is to write that list down somewhere you will see it again.

START HERE

Backups and multi-factor authentication

These two come first, whatever else is on your list. A backup you have never restored is only a hope, and an account protected by a password alone is one guess away.

THEN

Work outwards from there

Leavers and admin rights next, then devices and updates. Phishing and contracts can follow over the next month or two, once the basics are steady.

If it would help to have a second pair of eyes, we offer a free 20-minute review. We will go through your list with you, tell you honestly what matters most for a business your size, and leave you with a short plan you can act on. Plain English, no jargon, and no obligation.

Book your free 20-minute review

Send this checklist back to us, or simply get in touch and say you would like the review. We will find a time that suits you.

www.designmagic.net

Design Magic is a Kent-based IT support company helping businesses across the South East with IT support, cyber security, cloud, Microsoft 365 and Google Workspace.