IT Security Checklist for Small Businesses

24 points to self-assess the state of your IT security.

> How to use it: tick every item you can confidently answer with "yes". Open items are your priorities. This list is a first orientation and replaces neither a penetration test nor legal advice.

1. Access & passwords

- [ ] Every service has its own long password (a password manager is in use).
- [ ] Multi-factor authentication is enabled for email, cloud services and administrator accounts.
- [ ] Passkeys or hardware keys are used instead of passwords where possible.
- [ ] Default passwords on routers, printers and cameras have been changed.

2. Updates & software

- [ ] Operating systems, browsers and applications update automatically.
- [ ] Devices and software without vendor support are replaced or isolated.
- [ ] There is an inventory of all devices, applications and cloud services in use.
- [ ] Unneeded programs and user accounts are removed.

3. Backups

- [ ] Important data is backed up regularly; at least one copy is kept separate from the network (offline or immutable).
- [ ] Restoring has been tested in practice at least once.
- [ ] It is defined which data must be restored and how quickly.

4. Email & staff

- [ ] Staff know how to spot phishing and whom to report suspicious mail to.
- [ ] Payment instructions and bank detail changes require confirmation through a second channel (e.g. a call-back).
- [ ] There is a clear rule on which AI services may be used with which data.
- [ ] Nobody runs commands that a web page asks them to copy and paste.

5. Devices & network

- [ ] Laptops and smartphones are encrypted and locked with a PIN or biometrics.
- [ ] Current antivirus or an endpoint solution runs on all devices.
- [ ] Wi-Fi uses WPA2/WPA3; guests use a separate network.
- [ ] Remote access (VPN, remote desktop) is secured and not openly reachable from the internet.

6. Permissions & incident response

- [ ] Staff only have the access rights they need for their work.
- [ ] Access is revoked on the same day an employee leaves.
- [ ] An incident plan states whom to call and what to do first.
- [ ] Reporting duties (e.g. GDPR, NIS2) have been assessed and the responsible person knows them.
- [ ] Your website and systems have been tested by an independent party at least once.

How many items are open? I am happy to discuss where the biggest lever is in a free 20-minute intro call.
christian-noack.com/en/contact.html · admin@christian-noack.com