

ONIXED

27-Point IT Security Checklist

The exact checklist we use when assessing SMEs. Twenty minutes to work through. Could save you thousands.

Passwords & access

- 01 ☐ Default router and firewall passwords have been changed from factory settings.
-
- 02 ☐ Staff use unique passwords for every business account, not one password reused everywhere.
-
- 03 ☐ A password manager is used across the business instead of passwords in a spreadsheet or notebook.
-
- 04 ☐ Multi-factor authentication (MFA) is enabled on email and other critical accounts.
-
- 05 ☐ Staff access is reviewed and removed promptly when someone leaves the business.
-

Network & devices

- 06 ☐ Staff and guest WiFi run on separate networks.
-
- 07 ☐ Firewall rules are documented and reviewed, not left as whatever was configured on day one.
-
- 08 ☐ All devices have up-to-date antivirus or endpoint protection installed.
-
- 09 ☐ Operating systems and software are set to auto-update, or patched on a regular schedule.
-
- 10 ☐ Unused ports, services, and old accounts have been disabled.
-

Email & phishing

- 11 ☐ Staff have received phishing awareness training in the last 12 months.
-
- 12 ☐ Email filtering is in place to catch spam and malicious attachments.
-
- 13 ☐ There's a clear process for staff to report suspicious emails.
-
- 14 ☐ Financial requests received by email are verified through a second channel, such as a phone call.
-

Backups & recovery

- 15 ☐ Backups run automatically, not manually and inconsistently.
- 16 ☐ Backups are actually tested by restoring data, not just assumed to work.
- 17 ☐ At least one backup copy is stored offsite or in the cloud, separate from your main systems.
- 18 ☐ A basic incident response plan exists for what to do if something goes wrong.

Data & compliance

- 19 ☐ You know what personal data you hold and why you hold it.
- 20 ☐ A privacy policy is published on your website and kept up to date.
- 21 ☐ Data is only kept for as long as necessary, not indefinitely by default.
- 22 ☐ Third-party tools handling customer data are GDPR compliant.
- 23 ☐ You're registered with the ICO, if your business is required to be.

Physical & policy

- 24 ☐ Screens lock automatically when a device is left unattended.
- 25 ☐ Sensitive documents are stored securely, not left out on desks.
- 26 ☐ There's a written policy covering personal devices used for work (BYOD).
- 27 ☐ IT responsibility is clearly assigned to someone, even if the work itself is outsourced.

Ticked fewer than you'd like?

That's exactly what a free IT review is for. 30 minutes, no obligation, and we'll tell you honestly what to prioritise first.

support@onixed.co.uk · [07488 304127](tel:07488304127) · onixed.co.uk