SENTIS
Managed Solutions

Cybersecurity checklist

How secure is your business? Let's find out.

Cybersecurity is a business-critical issue. This quick checklist will help you work out your organisation's existing level of protection and highlight areas that need attention.

Tick "Yes" if you've got it covered, choose "Not sure" if it needs checking and select "no" if it's something you haven't already implemented. Each "Yes" answer is worth one point, while "Not sure" gives you 0.5 and "No" is zero.

This checklist takes around five minutes to complete. At the end, add up your total score to see how resilient your business is – and what to do next about online security.

To enable interactivity, please open in Chrome or Adobe Acrobat.

Policies and leadership

	Yes	No	Not Sure
• Do you have clear, documented information about security and privacy policies?	☐	☐	☐
• Are these policies regularly reviewed and updated?	☐	☐	☐
• Is a member of your leadership team accountable for cybersecurity?	☐	☐	☐
• Are there policies covering remote access, mobile devices and USB use?	☐	☐	☐
• Are internet, email and communications in place and followed?	☐	☐	☐
• Does senior IT leadership meet regularly with executives to discuss cybersecurity?	☐	☐	☐

Staff awareness and training

	Yes	No	Not Sure
• Is cybersecurity training included in onboarding for all staff?	☐	☐	☐
• Are regular refresher sessions provided for all employees?	☐	☐	☐
• Do staff know how to spot phishing or social engineering attacks?	☐	☐	☐
• Are simulated phishing or awareness tests used to assess staff knowledge?	☐	☐	☐

Access control and password management

	Yes	No	Not Sure
• Do users have unique login credentials?	☐	☐	☐
• Are admin privileges restricted to those who genuinely need them?	☐	☐	☐
• Are strong password policies enforced (e.g. length, complexity, renewal)?	☐	☐	☐
• Is multi-factor authentication (MFA) in place for key systems?	☐	☐	☐
• Are unused accounts disabled or deleted promptly?	☐	☐	☐

SENTIS
Managed Solutions

Cybersecurity checklist

Device and network security

	Yes	No	Not Sure
• Is antivirus or endpoint protection software installed on all devices?	☐	☐	☐
• Are firewalls and intrusion detection/prevention systems active?	☐	☐	☐
• Is your Wi-Fi network secured and segmented where appropriate?	☐	☐	☐
• Do you have secure methods for sending sensitive data?	☐	☐	☐
• Are servers and critical systems monitored for unusual activity?	☐	☐	☐

Data management and protection

	Yes	No	Not Sure
• Is sensitive data classified by type, risk and access level?	☐	☐	☐
• Are access rights granted on a need-to-know basis?	☐	☐	☐
• Is all data regularly backed up?	☐	☐	☐
• Are backups encrypted and stored securely offsite or in the cloud?	☐	☐	☐
• Is legacy or end-of-life software avoided or isolated?	☐	☐	☐

Incident response and recovery

	Yes	No	Not Sure
• Do you have a documented disaster recovery and incident response plan?	☐	☐	☐
• Is it tested and updated regularly?	☐	☐	☐
• Can you restore business operations within 48 hours of an attack?	☐	☐	☐
• Are penetration tests or vulnerability scans carried out regularly?	☐	☐	☐
• Are unsuccessful attack attempts logged, reviewed and investigated?	☐	☐	☐

Total score 0

Clear Form

SENTIS
Managed Solutions

Cybersecurity checklist

What your score means

25-30 – Cyber-savvy:

You've got solid foundations in place – but cyber threats are evolving all the time and ongoing vigilance is essential. Consider a professional cybersecurity health check to uncover any hidden weaknesses.

17-24.5 – Cause for concern:

There are clear gaps in your cybersecurity posture. You should take immediate steps to address them, starting with a formal risk assessment.

16.5 or below – Vulnerable:

Your organisation is exposed to significant risk. Even small fixes – like securing accounts and updating software – can make a big difference. Act now and seek expert support to protect your business.

Want a deeper analysis of your cyber defences? Book a Sentis cybersecurity health check. We'll assess your IT systems, identify vulnerabilities and provide you with a clear action plan. Visit our website at sentisms.com for more information.