INTOUCH TECH

Cyber Essentials Readiness Checklist

FIREWALL & BOUNDARY SECURITY

Your business must control traffic coming in and out of your network.

- □ A business-grade firewall is installed and configured
- □ Only required ports/services are open
- □ Remote access is protected (VPN + MFA)
- □ Firewall rules are reviewed regularly

SECURE CONFIGURATION

Devices must be set up securely. Not left on default settings.

- □ Default passwords have been removed from all systems
- □ Unnecessary software and services are disabled
- □ Devices follow secure configuration standards
- □ Admin privileges are restricted to authorised staff only

USER ACCESS CONTROL

Cyber Essentials requires strong access management.

- □ Each employee has their own unique login account
- □ No shared admin accounts are used
- □ Strong password policies are enforced
- □ Multi-Factor Authentication (MFA) is enabled for key services
- □ Leavers' accounts are removed immediately

MALWARE PROTECTION

You must protect against viruses, ransomware and malicious downloads.

- □ Antivirus or endpoint protection is installed on all devices
- □ Threat protection is actively monitored and updated
- □ Staff cannot install unauthorised applications
- □ Email filtering is in place to reduce phishing risk

INTOUCH TECH

PATCH MANAGEMENT & UPDATES

One of the most common reasons businesses fail Cyber Essentials.

- □ All devices run supported operating systems
- □ Windows and macOS updates are applied regularly
- □ Patch compliance is tracked centrally
- □ Critical updates are applied within 14 days

DEVICE & REMOTE WORKING SECURITY

Remote work is included in Cyber Essentials scope.

- □ Company laptops are encrypted
- □ Lost/stolen devices can be remotely wiped
- □ Staff do not use unmanaged personal devices for work
- □ Remote access tools are secured and approved

BACKUP & RECOVERY READINESS

Backups aren't mandatory in the standard, but they reduce risk massively.

- □ Backups are running automatically
- □ Backups are stored securely and separated from main systems
- □ Recovery tests are completed regularly
- □ Ransomware recovery plan exists

STAFF AWARENESS & PHISHING DEFENCE

Most cyber incidents start with human error.

- □ Staff understand phishing and suspicious emails
- □ Security awareness training is delivered at least annually
- □ Users know how to report cyber concerns quickly
- □ MFA is used to reduce credential theft risk

Want us to check this with you?
Book a **FREE** 15-minute call with our **In-House Cyber Team.**

hello@intouchtech.co.uk **03333 707 000**