INTOUCH TECH

Cyber Security & Compliance

Cyber Essentials Readiness Checklist

Use this checklist to assess your readiness for Cyber Essentials certification. Tick each item as you confirm compliance. For expert guidance through the certification process, contact Intouch Tech.

1 Firewalls & Internet Gateways

- [ ] A firewall is installed at the boundary of your network(s)
- [ ] Default firewall admin passwords have been changed
- [ ] Firewall rules are documented and approved by an authorised person
- [ ] Unnecessary firewall rules have been removed or disabled
- [ ] Firewall management interfaces are not accessible from the internet
- [ ] Host-based firewalls (software firewalls) are enabled on all devices
- [ ] Inbound firewall rules only permit traffic that is needed for business purposes
- [ ] Home workers use software firewalls or VPN-secured connections

2 Secure Configuration

- [ ] Default passwords on all devices and software have been changed
- [ ] Unnecessary user accounts have been removed or disabled
- [ ] Auto-run / auto-play features are disabled
- [ ] Password policy enforces a minimum of 8 characters (or 12+ for admin accounts)
- [ ] Multi-factor authentication (MFA) is enabled where available
- [ ] Account lockout or throttling is configured after no more than 10 failed login attempts
- [ ] Unnecessary software and services have been removed or disabled
- [ ] Devices are configured to lock after a defined period of inactivity

3 Security Update Management

- [ ] All software and operating systems are licensed and supported by the vendor
- [ ] Automatic updates are enabled where possible
- [ ] Critical and high-severity patches are applied within 14 days of release
- [ ] Unsupported software has been removed or isolated from the network
- [ ] A process is in place to identify and apply updates to firmware
- [ ] You maintain an inventory of all software in use across the organisation

4 User Access Control

- [ ] User accounts are assigned on an individual basis (no shared accounts)
- [ ] Admin/privileged accounts are only used for administrative tasks
- [ ] Standard user accounts do not have admin privileges
- [ ] A documented process exists for creating, approving, and removing user accounts
- [ ] Leavers' accounts are disabled or removed promptly
- [ ] Access to data and services is limited based on business need (least privilege)
- [ ] All user accounts are protected by passwords or equivalent authentication
- [ ] MFA is enabled on all cloud services and externally accessible admin accounts

5 Malware Protection

- [ ] Anti-malware software is installed on all in-scope devices
- [ ] Anti-malware software is configured to update automatically (at least daily)
- [ ] Anti-malware is configured to scan files on access and when downloaded
- [ ] Anti-malware is set to prevent connections to malicious websites
- [ ] Users are prevented from running unapproved applications (if using application allow-listing)
- [ ] A sandbox or equivalent is used to test untrusted content where applicable

6 General Readiness & Scope

- [ ] You have identified all devices, software, and accounts in scope for the assessment
- [ ] BYOD (Bring Your Own Device) policies are documented if personal devices access company data
- [ ] Cloud services (e.g. Microsoft 365, Google Workspace) are included in scope
- [ ] You have a clear understanding of your network boundary
- [ ] Third-party IT providers have confirmed they meet Cyber Essentials requirements for managed services
- [ ] You have identified who in your organisation will complete or oversee the assessment

Notes

Ready to get certified?

Intouch Tech guides you through every step of the Cyber Essentials certification process.

Get in touch today to start your certification journey.