Cyber Essentials Checklist

Contents

1. Introduction

At BlackBox Pentesters**,** we believe cybersecurity should be accessible to everyone. Every organisation deserves clear, practical guidance that helps them build strong foundations and understand what good security looks like in the real world.

This free Cyber Essentials guide was created to give you a straightforward, easy-to-use checklist that supports you in strengthening your environment and preparing for certification. No complexity. No unnecessary barriers. Just the essential controls presented in a simple, actionable format.

Use this guide to review your infrastructure, close any gaps, and build a resilient security posture. Whether you're working toward Cyber Essentials, Cyber Essentials Plus, or simply looking to enhance your organisation’s defences, this provides a solid starting point.

2. Checklist

1. Firewalls & Internet Gateways

- All internet-connected devices are protected by a firewall ☐
- Default admin passwords on firewalls replaced with strong unique credentials ☐
- Unnecessary ports closed; only required inbound/outbound rules allowed ☐
- Remote management disabled or locked to specific IPs ☐
- Firewall software/firmware fully updated ☐
- NAT or equivalent shielding active on routers ☐

2. Secure Configuration

- Default usernames removed/disabled ☐
- Default passwords changed ☐
- Unnecessary software removed (bloat, trialware, legacy apps) ☐
- Auto-run/autorun disabled ☐
- Local admin accounts restricted and unique per machine ☐
- Secure boot enabled where supported ☐
- BIOS/UEFI protected with a strong password ☐

3. User Access Control

- Users only have access necessary for their role (least privilege) ☐
- Admin accounts used **only** for admin tasks (no email/browsing) ☐
- MFA enabled for all cloud services ☐
- Unique credentials for each user (no shared accounts) ☐
- Leavers' accounts disabled or deleted immediately ☐
- Strong password policy enforced (length > complexity preference) ☐

4. Malware Protection

- Anti-malware installed and active on all devices ☐
- Real-time protection enabled ☐
- Automatic scanning and definition updates switched on ☐
- Only trusted apps allowed to run (whitelisting/AppLocker) ☐
- Users blocked from installing unapproved software ☐
- Devices protected against malicious macros ☐

5. Patch Management

- Operating systems fully up to date ☐
- Critical and high-risk patches installed within 14 days ☐
- Unsupported OS or software removed or isolated ☐
- Automatic updates enabled ☐
- Third-party apps included in patching cycle ☐
- Hardware firmware updates reviewed regularly ☐

Device & Asset Scope (required for Cyber Essentials)

- Full asset list documented (laptops, desktops, mobiles, cloud apps) ☐
- List shows which devices are **in scope** for assessment ☐
- Work-from-home devices included if used for business ☐
- Personal/BYOD devices controlled or restricted ☐

Cloud Services (M365, Google Workspace, etc.)

- MFA enforced for **all** users ☐
- Security defaults or baseline policies enabled ☐

- Unused services/apps disabled ☐
- Admin access locked down and monitored ☐
- External sharing policies reviewed and restricted ☐
- Audit logs enabled ☐

Network & Remote Working

- Home routers either company-controlled or verified secure ☐
- VPN protected with strong encryption ☐
- Guest networks separated from internal systems ☐
- Wi-Fi using WPA2/WPA3 only ☐
- Default Wi-Fi router credentials changed ☐

Documentation Required for Certification

- Incident response plan ☐
- Access control policy ☐
- Patch management process ☐
- Firewall and configuration policy ☐
- Asset register ☐
- Supplier/cloud service list ☐