IT CLUB KNOWLEDGE CENTRE

Cyber Essentials Readiness Checklist

Review the five control areas before you apply

1. Scope

- [ ] List all devices and cloud services
- [ ] Include personal (BYOD) devices
- [ ] Identify unsupported operating systems

2. Firewalls

- [ ] Firewall on every internet connection
- [ ] Default router passwords changed
- [ ] No exposed firewall administration
- [ ] Unused inbound rules removed

3. Secure Configuration

- [ ] Unused software and accounts removed
- [ ] Auto-run from removable media off
- [ ] Device locking enforced
- [ ] Default passwords changed

4. User Access Control

- [ ] Individual accounts — no shared logins
- [ ] Separate administrator accounts
- [ ] MFA on all cloud services
- [ ] Leavers' accounts removed promptly

5. Malware Protection

- [ ] Anti-malware on every device
- [ ] Automatic updates and on-access scanning
- [ ] Malicious websites blocked

6. Security Updates

- [ ] All software licensed and supported
- [ ] Automatic updates enabled
- [ ] Critical updates applied within 14 days
- [ ] Unsupported software removed

7. Before You Submit

- Record evidence for each control area
- Fix the gaps — do not certify around them
- Choose Cyber Essentials or Cyber Essentials Plus
- Pick an IASME-accredited certification body
- Diarise annual recertification

Scan for the full guide

itclub.work/knowledge-centre

Five control areas. Close the gaps before you apply.

IT Club

Technology Intelligence — Plain-English guidance for business owners

https://itclub.work/knowledge-centre