



Cyber Essentials Readiness

A practical walkthrough of the five Cyber Essentials controls. One-page summary.

The 10 things to remember

- 1 Cyber Essentials is a baseline against common, opportunistic attacks, not every threat.
- 2 Base certification is a verified self-assessment; Plus adds independent technical testing.
- 3 Change every default password, on every device, before it goes into use.
- 4 Block inbound connections by default; only open ports with a documented business need.
- 5 Harden devices: remove unused software and accounts, disable auto-run, enable auto-lock.
- 6 Patch critical and high severity vulnerabilities within 14 days of release.
- 7 Replace or upgrade end-of-life software; unsupported means unpatched forever.
- 8 Give admin rights only to those who need them, and never for everyday email and browsing.
- 9 Use MFA for cloud services and all administrative accounts; it has been mandatory since 2022.
- 10 Disable leavers' accounts promptly and re-certify every twelve months.