

Cyber Essentials

Guard against cyber threats and demonstrate your commitment to cyber security



As reliance on internet technologies increases, so do the opportunities for criminals and hackers to commit fraud, industrial espionage or the theft of intellectual property. Cyber Essentials defines a set of five key security controls which, when properly implemented, will better protect businesses – small and large – from attacks using software and techniques which are freely available on the open internet.

Designed to be light-touch and achievable at low cost, Cyber Essentials provides a clear statement of five basic security controls that, when properly implemented, will reduce your risk from cyber threats and will help protect you from 80% of cyber-attacks.

Tel 0345 – 646 1050

info@softworx.co

www.softworx.co

What is Cyber Essentials?

Cyber Essentials is a Government-backed and industry supported scheme to help you protect your organisation from cyber threats and demonstrate your commitment to cyber security. It defines a set of five key security controls that organisations should implement, as a minimum, to reduce the risk of cyber threats.

The five key controls are:

- **Boundary Firewalls & Gateways** – use devices designed to prevent unauthorised access to or from private networks
- **Secure Configuration** – ensure that systems are configured in the most secure way for the needs of the organisation
- **Access Control** – ensure only those who should have access to systems are provided access at an appropriate level
- **Malware Protection** – ensure that virus and malware protection is installed and up to date
- **Patch Management** – ensure the latest supported version of applications is used, and all patches and updates applied

Cyber Essentials Basic or Cyber Essentials Plus?

Cyber Essentials offers two levels of certification:

Cyber Essentials Basic – basic level of certification is awarded based on a completed self-service questionnaire, which is assessed by us.

Cyber Essentials Plus – is a higher level of assurance and we will work with you to test that the five key controls covered by Cyber Essentials Basic are working in practice with simulated hacking and phishing attacks.



Get in touch today

0345 – 646 0150

info@softworx.co www.softworx.co

Government's Cyber Resilience Strategy

On 8th November 2017, the Government published its Public Sector Action Plan on Cyber Resilience. It sets out the key actions that the Government, public bodies and key partners will take up to the end of 2018 to further enhance cyber resilience in public sector. Key Action asks that public bodies ensure they are Cyber Essentials Plus certified by end of October 2018.

Why consider Cyber Essentials?

- Prevent common cyber attacks which use freely available software and techniques
- Identify areas for improvement even if your company has a proven track record of good security
- Reassure your customers that you are taking the necessary steps to secure their sensitive data
- The supply chain within Public Sector is changing and the requirement for Cyber Essentials certification is becoming more prevalent
- Display the Cyber Essentials badge to demonstrate that you take cyber security seriously by adhering to a widely-endorsed standard
- Achieving Cyber Essentials accreditation can assist with preparing for GDPR
- Cyber insurance agencies often look more favourably on organisations that have achieved Cyber Essentials certification
- When maintained correctly, Cyber Essentials will stop 80% of cyber attacks

Why Softworx?

Our consultants are accredited by IASME to assess and certify against the Government's Cyber Essentials scheme requirements and offer consulting services to help organisations achieve Cyber Essentials certification



Get in touch today

0345 – 6460150

Glasgow - Durham - Manchester

www.softworx.co