



Cyber Essentials certification:

What you need to know

www.select-technology.co.uk

What is Cyber Essentials?

Cyber Essentials is a simple but effective government-backed scheme that will help you to protect your organisation against a whole range of the most common cyber-attacks.

Key features of Cyber Essentials

-  It's a government backed scheme
-  Annual certification, renewable every 12 months
-  For all business sizes, UK or overseas
-  Required for many commercial and government contracts
-  Two levels of certification - Cyber Essentials and Cyber Essentials Plus



The benefits of Cyber Essentials certification

- Prove to customers that cyber security is a priority in your organisation.
- Stay ahead of new cyber security risks by assessing your systems against a recognised framework each year.
- Apply for the growing number of contracts that address supply chain security with Cyber Essentials certification
- Cyber Essentials certification includes automatic cyber liability insurance for any UK organisation who certifies their whole organisation and has less than £20m annual turnover.

67%

of companies reported a cyber-attack in the past 12 months according to leading insurer, Hiscox.

92%

fewer insurance claims are made by organisations with the Cyber Essentials controls in place, according to the UK's National Cyber Security Centre.

Cyber Essentials

The five security protocols

Cyber Essentials represents the UK Government's minimum baseline standard for cyber security for organisations of all sizes in the UK. The certification scheme is aligned to five technical controls designed to prevent the most common internet-based cyber security threats.



Boundary firewalls and internet gateways

Internet gateways and firewalls will identify and prevent unwanted traffic gaining access to your network, computers and systems.



Secure Configuration

Default factory settings on new computers or software are not secure. These settings prioritise quick and easy operation, leaving systems vulnerable to cyber risks. Configuring all computers and network devices properly is essential to reduce these risks.



Access Control

Many data and cyber breaches occur from abuse of administrative user accounts. Organisations and businesses should aim to only allow certain individuals special access privileges according to their position and responsibilities.



Malware Protection

Computers and systems need to be protected from malware. Malware is a programme, or virus, that has been coded with the intent to perform unauthorised actions on one or more computers. Organisations should, at a minimum, look to protect all computers that are connected to the internet via cable or wireless.



Patch Management

As with any software, there are often regular updates released to add features, improve performance, and resolve discovered vulnerabilities. If there are any vulnerabilities in software that haven't been updated, this can be used to gain elevated or unauthorised access to networks and computer systems.

How to apply for Cyber Essentials

At the first level of Cyber Essentials, organisations assess themselves against the five basic security controls via an online questionnaire which is then verified by a qualified assessor based on the information provided. You can achieve certification with 2 or fewer major non-conformances.

Cyber Essentials Plus is the next step, it requires an independent verification of everything that was claimed in Cyber Essentials from a certified body, alongside an in-depth vulnerability scanning process. This extra level of scrutiny means your Cyber Essentials Plus certification will hold more weight with potential customers.

Our approach to Cyber Essentials accreditation

We are committed to providing a thorough and supportive service that is tailored to the needs of each client.

Most other providers only verify (mark) your assessment. This can leave you with a list of gaps that you're unable to address quickly enough to pass the assessment. Our approach is different. Our cybersecurity expert will spend time with you from the starts to ensure your successful accreditation. We will support with:

- Defining the scope of your assessment
- Identifying your assets
- Identifying technical and policy gaps
- Engaging with your third-party vendors
- Developing remediation strategies



Doing all of this as part of the assessment process ensures that you are fully prepared to meet the assessment criteria and address gaps with adequate time and resources. After all there's nothing worse than completing a piece of work only to find out that it didn't make the grade, and you'll need to pay again to re-submit.

If you are already a Select Technology managed service customer a number of remediation tasks will be completed under that agreement, so you won't be required to pay for those works either.

“Achieving Cyber Essentials certification was an essential step for our business development. Select Technology guided us through the certification process and ensured we complied with all the standards.”

Simon Lester, Jarvis Tech



To find out more about **Cyber Essentials** just drop us a line hello@select-technology.co.uk or give us a call **01892 830 111**.

www.select-technology.co.uk

01892 830 111

hello@select-technology.co.uk

4 Cannon Park, Transfesa Road,
Paddock Wood, Kent, TN12 6UF

