CYBER ESSENTIALS
A JARGON FREE GUIDE

Brought to you by Assure Technical

Get in touch with our cyber experts

Telephone: +44 (0)1684 252 770

Email: cyber@assuretechnical.com

www.assuretechnical.com

CYBER ESSENTIALS

CYBER ESSENTIALS
WHAT IS IT?

Cyber Essentials is the government-backed cyber accreditation scheme that sets out a standard baseline for cyber security.

Launched in response to a growing cyber threat, it protects all organisations that use internet connected end-user devices or systems.

It's specifically designed to provide a straightforward and affordable approach to cyber security.

CYBER ESSENTIALS
THE KEY BENEFITS

Protection from Cyber Attack

Protect your organisation from up to 80% of IT security breaches

Meet Tender Requirements

Gain access to UK Government contracts and a growing number of Commercial contracts that enforce Cyber Essentials supply chain requirements

Reassure Your Key Stakeholders

Demonstrate that you have robust information security measures in place and comply with a Government recognised standard

GDPR Readiness

Help your business address compliance requirements such as the EU General Data Protection GDPR Regulation

Cyber Liability Insurance

Automatic £25,000 indemnity cover for organisations with a turnover less than £20m (terms apply)

ASSURE
technical

KEY REQUIREMENTS
THE FIVE BASICS CONTROLS

Cyber Essential certification is awarded to organisations who can demonstrate, through the completion of a self assessment questionnaire, that they have implemented five basic cyber security controls.

1 Use a firewall to secure your Internet connection

You should protect your Internet connection with a firewall. This effectively creates a 'buffer zone' between your IT network and other, external networks and the internet.

Within this buffer zone, incoming traffic can be analysed to find out whether or not it should be allowed onto your network.

Two types of firewall

It is possible to use a personal firewall on your internet connected computer (normally included within your Operating System as standard).

If you have a more complicated set up with many different types of devices, you might require a dedicated boundary firewall, which places a protective buffer around your network as a whole.

Some routers will contain a firewall, which could be used in this boundary protection role. But, this can't be guaranteed - ask your internet service provider about your specific model.

Cyber Essentials Certification...

Cyber Essentials Certification requires that you use and configure a firewall to protect all your devices, particularly those that connect to public or other untrusted Wi-Fi networks.

2 Choose the most secure settings for your devices and software

Manufacturers often set the default configurations of new software and devices to be as open and multi-functional as possible. They come with 'everything on' to make them easily connectable and usable.

Unfortunately, these settings can also provide cyber attackers with opportunities to gain unauthorised access to your data, often with ease.

Check the settings

You should always check the settings of new software and devices and where possible, make changes, which raise your level of security. For example, by disabling or removing any functions, accounts or services that you do not require.

Use passwords

Your laptops, desktop computers, tablets and smartphones contain your data. They also store the details of the online accounts that you access, so both your devices and your accounts should always be password-protected.

Passwords - when implemented correctly - are an easy and effective way to prevent unauthorised users accessing your devices. Passwords should be easy to remember and hard for somebody else to guess.

The default passwords on new devices such as 'admin' and 'password' are the easiest of all for attackers to guess. Therefore, you must change all default passwords before devices are distributed and used. The use of PINs or touch-ID can also aid device security.

Extra Security

For 'important' accounts, such as banking and IT administration, you should use two-factor authentication, also known as 2FA. A common and effective example of this involves a code being sent to your smartphone which is entered in addition to your password.

Cyber Essentials Certification...

requires that only necessary software, accounts and apps are used.

3 Control who has access to your data and services

To minimise the potential damage that could be done if an account is misused or stolen, staff accounts should have just enough access to software, settings, online services and device connectivity functions for them to perform their role. Extra permissions should only be given to those who need them.

Administrative accounts

Check what privileges your accounts have - accounts with administrative privileges should only be used to perform administrative tasks. Standard accounts should be used for general work.

By ensuring that your staff don't browse the web or check emails from an account with administrative privileges you cut down on the chance that an admin account will be compromised.

This is important because an attacker with unauthorised access to an administrative account can be far more damaging than one accessing a standard user account.

Cyber Essentials Certification...

requires that you control access to your data through user accounts, that administration privileges are only given to those requiring them, and that administrator privileges are controlled.

4 Protect yourself from viruses and other malware

Malware is software or web content that has been designed to cause harm. For example, the WannaCry attack used a form of malware which makes data or systems unusable until the victim makes a payment.

Viruses are the most common form of malware. These programs infect legitimate software, make copies of themselves and send these duplicates to any computers that connect to their victim.

How malware works

There are various ways in which malware can find its way onto a computer. A user may open an infected email, browse a compromised website or open an unknown file from removable storage media, such as a USB memory stick.

Three ways to defend against malware:

1. Antivirus software is often included for free within popular operating systems. It should be used on all computers and laptops. Enabling this on your office equipment will make you instantly safer from attack.
2. You should only download apps for mobile phones and tablets from manufacturer-approved stores (like Google Play or Apple App Store). These apps are checked to provide a certain level of protection from malware. You should prevent staff from downloading apps from unknown vendors/sources, as these will not have been checked.
3. For those unable to install antivirus or limit users to approved stores, there is another, more technical, solution. Apps and programs can be run in a ‘sandbox’. This prevents them from interacting with, and harming, other parts of your devices or network.

Cyber Essentials Certification...

requires that you implement one of the three malware defence approaches listed here.

5 Keep your devices and software up to date

No matter which phones, tablets, laptops or computers your organisation is using, it’s important they are kept up to date at all times. This is true for both Operating Systems and installed apps or software. Doing so is quick, easy, and free.

Manufacturers and developers release regular updates, which not only add new features, but also fix any security vulnerabilities that have been discovered.

Applying these updates (a process known as patching) is one of the most important things you can do to improve security. Operating systems, software, devices and apps should all be set to ‘automatically update’ wherever this is an option. This way, you will be protected as soon as the update is released.

However, all IT has a limited lifespan. When new updates cease to appear for your hardware or software, you should consider a modern replacement.

Cyber Essentials Certification...

requires that you keep your devices, software and apps up to date.

ON THE RIGHT PATH
YOUR CYBER ESSENTIALS JOURNEY

Once you have taken the time to investigate these five basic controls and put them in place, you and your organisation will be on the right path for gaining Cyber Essentials Certification.

Ready to take your first steps?

Assure Technical has been an IASME Accredited Certification Body in 2017. Since then, we have certified hundreds of organisations from a wide range of industries. Our competitive prices, quick turnarounds and pragmatic approach will help ensure you achieve Cyber Essentials with ease. To get started, simply select the package that best suits your budget, timeframe and needs.

Three Simple Steps

1. Answer a series of questions about your current cyber controls via the Assure Technical Portal.
2. Our experts will check your questionnaire responses, advising of any changes that need to be introduced. We may ask for evidence to support your answers.
3. Your Cyber Essentials Report and Certificate will be issued as soon as you have met all of the Questionnaire criteria.

Whether you feel able to complete your self assessment questionnaire independently, require specialist guidance to pass first time, or are looking for a trusted supplier to deliver a turnkey solution on your behalf, we have a range of Cyber Essentials Packages to suit your budget, timeframe and level of experience.

DIY Package **£300**	**Supported Package** **£545**	**Turnkey Solution** **From £1,245**
Cyber Essentials Certification	Cyber Essentials Certification (worth £300)	Cyber Essentials Certification (worth £300)
Straightforward, secure online self assessment process	Unlimited remote support throughout your journey to certification	We manage the certification process on your behalf
Submit details about your current cyber security measures	Same day assessments for submissions made before 3pm	Minimise your internal workload. Quick turnarounds. Pass first time.
Our cyber experts assess your submission quickly	Pass first time with our pre-submission review and feedback	We conduct a remote cyber audit and guide you through any required changes
Includes 1 complimentary re-test within 7 days of your initial submission	Straightforward, secure online self assessment process	We complete the Cyber Essentials Questionnaire ready for your approval

The prices listed are exclusive of VAT and available to Small & Medium size organisations only. Full terms and conditions apply.
Bespoke Quotations available on request.

PAY SECURELY ONLINE

Cyber Essentials PLUS

Cyber Essentials PLUS is awarded to organisations when the evidence provided in their basic Cyber Essentials self assessment is audited through a series of vulnerability tests.

We provide competitively priced Cyber Essentials PLUS certifications that can be delivered as a standalone service, or in combination with basic Cyber Essentials.

Our experienced assessors will work in partnership with you and offer pragmatic support to help you achieve certification quickly, whilst minimising impact on your internal resource.

Key Cyber Essentials PLUS Benefits

- Reassure your stakeholders that the IT security measures you have put in place to safeguard your services and data meet the UK Government benchmark and have been externally audited
- Displaying the Cyber Essentials PLUS mark provides you with a competitive advantage when attracting and retaining customers
- Cyber Essentials PLUS is a key requirement for Government, Defence and Critical National Infrastructure sector contracts
- A growing number of Commercial sector organisations are now stipulating that their supply chain have Cyber Essentials PLUS in place

Our Cyber Essentials PLUS audits can be conducted 100% remotely whilst individuals work from home.

Why Choose Us?

Assure Technical provide competitively priced Cyber Essentials PLUS assessments. We have a proven track record in delivering honest, jargon free advice and support.

We will work in partnership with you and adopt a pragmatic approach to help you achieve certification quickly, whilst minimising impact on your internal resource.

We can offer Cyber Essentials PLUS certifications in combination with Cyber Essentials basic, or as a standalone service (this is possible if you've obtained the basic Cyber Certification recently).

Our competitive rates, agile workforce and quick turnarounds ensure that our clients receive a great level of service.

Contact us today for a Same Day Quotation.

ASSURE
technical

www.assuretechnical.com