THE
CYBER
RESILIENCE
CENTRE
FOR THE **EAST MIDLANDS**

Cyber Essentials

CONTENTS

About Cyber Essentials

So far in your step-by-step information packs we've provided you with information about the cyber risks you need to consider, our free resources and our uniquely affordable services.

However, your cyber resilience journey isn't over. If you haven't already, it may now be time to consider achieving a level of cyber security assurance for your business.

This information pack goes through Cyber Essentials Certification to give you some insight into it. You'll also meet our Cyber Essentials Partners; who are highly skilled and friendly local Cyber security professionals who can guide you through the process and then certify your business as Cyber Essentials certified!

ABOUT CYBER ESSENTIALS

Cyber Essentials is a Government-backed and industry-supported scheme that helps businesses protect themselves against the growing threat of cyber attacks and provides a clear statement of the basic controls organisations should have in place to protect themselves.

It is the UK Government's answer to a safer internet space for organisations of all sizes, across all sectors. Developed and operated by the National Cyber Security Centre (NCSC), Cyber Essentials is considered the best first step to a more secure network, protecting you from 80% of the most basic cyber security breaches.

Gaining Cyber Essentials certification also enables organisations to showcase their credentials as trustworthy and secure when it comes to cyber security.

The certification defines a focused set of controls which provide clear guidance on basic cyber security for organisations of all sizes and offers a sound foundation of cyber security measures that all types of organisations can implement at a low cost.

There are two levels to the certification:

1. CYBER ESSENTIALS

This is a self-assessment option gives you protection against a wide variety of the most common cyber attacks. This is important because vulnerability to basic attacks can mark you out as target for more in-depth unwanted attention from cyber criminals and others.

Certification gives you peace of mind that your defences will protect against the vast majority of common cyber attacks simply because these attacks are looking for targets which do not have the Cyber Essentials technical controls in place.

Cyber Essentials shows you how to address those basics and prevent the most common attacks.

2. CYBER ESSENTIALS PLUS

Cyber Essentials Plus still has the Cyber Essentials trademark simplicity of approach, and the protections you need to put in place are the same, but for Cyber Essentials Plus a hands-on technical verification is carried out.

CYBER
ESSENTIALS

About Cyber Essentials

WHY SHOULD YOU GET CYBER ESSENTIALS?

Cyber hackers are becoming more intelligent and have adapted to many counter-hacking measures. Since 2017 the number of businesses experiencing phishing attacks has jumped from 72% to 86% (Cyber breaches survey 2020). There has never been a better time to become Cyber Essentials certified.

Cyber Essentials certification indicates that your organisation takes a proactive stance against malicious cyber attacks. In addition, it offers a mechanism to demonstrate to customers, investors, insurers and others that you have taken the minimum yet essential precautions to protect your organisation against cyber threats.

The National Cyber Security Centre states that undertaking the Cyber Essentials certification process and implementing even one of the five controls required by Cyber Essentials can protect businesses from around 80% of attacks.

Additional benefits of the certification include:

- Reassure customers that you are working to secure your IT against cyber attack
- Attract new business with the promise you have cyber security measures in place
- You have a clear picture of your organisation's cyber security level
- Some Government contracts require Cyber Essentials certification

The Five Controls of **Cyber Essentials**

1. FIREWALLS

The Firewall is a network security system that monitors and controls the various forms of network traffic that travel through your system daily – all based on predefined security rules. Firewalls are the barriers that separate your network from the internet. As the gatekeeper, it allows and disallows access.

By blocking unauthorised access to your network, firewalls prevent others from controlling your data or accessing your systems, while allowing secure access to those outside your network whom you do wish to allow access.

It is a MUST that all devices in your network have Firewall protection. To ensure that you are protected to the best possible standard, you should make some further considerations after you install your firewall software:

The presence of a firewall alone is not enough – you need to prove that you are blocking high-risk traffic as well.

Protect your Firewall configuration with strong passwords. It is recommended that administrators use long, complex passwords with numbers, letters, and punctuation – the more complex the password, the harder it will be to guess.

Devices used outside of the business network must be protected with a software firewall. Using remote working devices (your laptops, phones, and tablets) on high-risk networks (e.g., public Wi-Fi) requires technical security measures. In general, we recommend avoiding public Wi-Fi.

Firewalls

The Five Controls of **Cyber Essentials**

2. SECURE CONFIGURATION

Secure Configuration is the second of the five controls.

The goal is to make device and software settings as secure as possible. Proactive IT management is the key to achieving this goal.

As far as security is concerned, the default security settings on operating systems are never adequate to protect your system. To allow users to experience the new device as fluidly as possible, the factory settings are designed to be as unrestrictive as possible. Users can also customise the settings to suit their own needs.

For Cyber Essentials certification, settings must be reconfigured to ensure that higher levels of security are enforced.

Secure Configuration

The Five Controls of **Cyber Essentials**

3. APPLYING ACCESS CONTROLS

Access to data must be controlled. Access to administrative accounts needs to be controlled, and privileges should be granted only when absolutely necessary.

The user accounts in your business allow you to access all applications and devices, as well as sensitive information about your clients. Allowing only authorised personnel to have access to accounts that reflect their roles in the organisation greatly reduces the risk of damaging or stealing your data.

A breach of an account with privileged access to devices, applications, and information could have devastating consequences. Even worse, they could facilitate a large-scale attack at a later date, causing even more damage – financially, operationally, and reputationally.

Cyber Essentials certification requires the following:

- You have full control over all user accounts and the access privileges of each of them
- You must have user account creation and approval processes in place
- Users must be authenticated before granting access to application devices, and all credentials for each must be entirely unique
- Special access privileges to individual accounts must be removed when no longer required
- User accounts must be disabled when no longer required

Applying Access Controls

The Five Controls of **Cyber Essentials**

4. ANTI-MALWARE MEASURES

Make sure you take all necessary steps to prevent Malware from penetrating your systems. If you fail to do so, you will fall short of the standards required for Cyber Essentials accreditation.

Install software only from trusted sources. In the Apple App store and Google Play, for instance, whole teams of experts constantly monitor the apps for malware. Even though an unknown source may offer a cheap app, it could open the floodgates to malware.

It is essential that you protect every computer and device you use, both at home and at work, with anti-virus software. However, free anti-virus software on most operating systems is typically unable to protect your systems adequately since they are basic and offer little protection against modern, sophisticated cyber attacks.

Anti-Malware Measures

The Five Controls of **Cyber Essentials**

5. SYSTEM MAINTENANCE

Updating devices and software is essential, since using devices and software that have updates available but not installed leaves them vulnerable to security risks and prevents you from achieving Cyber Essentials certification.

Cyber Essentials takes a slightly lenient approach in this area. They require that you install updates within two weeks of their release if the vendor describes the patch as fixing 'high' or 'critical' flaws – at least that gives you time to prepare for the update, so you don't have to stop production immediately. In every case, you should ensure that your software is licensed, supported, and up-to-date. It is also necessary to remove all software from devices that are no longer supported.

If your business runs a piece of legacy software that is no longer being updated, but is still required, use a 'Sandbox'. The Sandbox stops your apps from communicating with other parts of your network, so they cannot be harmed.

System Maintenance

Meet our **Cyber Essentials Partners**

Hopefully by now you can see the logic of implementing those 5 controls, you may be able to do everything yourself. If you can check out the NSCC's Cyber Essentials Readiness Toolkit at *www.getreadyforcyberessentials.iasme.co.uk/questions/*

Ready to certify? Not ready? Need additional help? Not a clue and just want someone to do it all for you? Get in touch with us and we'll talk it through and introduce you to our Cyber Essentials partners.

Our Cyber Essentials Partners are official providers of the Cyber Essentials Certification.

Our partners have been accredited by the Information Assurance for Small and Medium Enterprises Consortium (IASME). With the accreditation from IASME, it allows our Cyber Essentials Partners to help your organisation achieve Cyber Essentials and Cyber Essentials Plus Certification.

Our Cyber Essentials Partners are also bound by our Code of Conduct. You can read our Code of Conduct at *www.emcrc.co.uk/code-of-conduct*

Meet our Cyber Essentials Partners at *www.emcrc.co.uk/cyber-essentials-partners*

Stay **Connected**

Our team at the EMCRC are friendly, knowledgeable and on hand for you to contact for support and guidance should you need us.

To stay up to date with the latest news from us and the wider security industry, please follow us on our social media channels.

FOLLOW US

LinkedIn

Twitter

Facebook

Instagram

In the coming weeks, we will be in touch to see how you are making use of the information and resources that we have provided to see if you need any additional support from us.

The Cyber Resilience Centre for the East Midlands is looking forward to working in partnership with you and your organisation to make the East Midlands region a more cyber resilient place to live, work and do business.

THE
CYBER RESILIENCE CENTRE
FOR THE **EAST MIDLANDS**

Reporting Cyber Crime

If you or someone else is in immediate danger or risk of harm dial 999 now.

Anyone can find themselves the victim of cyber crime.

If you are a business, charity or other organisation which is currently suffering a live cyber attack (in progress), call Action Fraud (0300 123 2040) immediately.

This service is available 24 hours a day, 7 days a week.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

REPORTING A CYBER ATTACK WHICH ISN'T ONGOING

Please report online to Action Fraud, the UK's national reporting centre for fraud and cybercrime. You can report cybercrime online at any time using the online reporting tool, which will guide you through simple questions to identify what has happened. Action Fraud advisors can also provide any help, support and advice you may need. Alternatively, you can call Action Fraud on 0300 123 2040 (textphone 0300 123 2050).

When you report a fraud to Action Fraud, you are given a police crime reference number and your case will be referred to the National Fraud Intelligence Bureau (NFIB), which is run by the police.

In some cases, the police and other law enforcement agencies may want to contact you for further details, so it's important that you provide your correct contact details and keep any relevant information about the crime.

Although the police cannot investigate every report individually, the information you provide will aid them. The police use your information to build up intelligence about cybercrime, which includes who is committing what crimes and against whom. This contributes to making the UK a more hostile place for cybercriminals to operate and helps to keep other potential victims safe.

When you report to Action Fraud, you can also choose to have your details passed on to Victim Support, a national charity that helps those affected by crime. If you take up this option, you will then be contacted by someone from the charity and offered free and confidential emotional support and practical help.

For more information on how to report different forms of cyber crime, visit ***www.emcrc.co.uk/reporting-cybercrime***

THE
CYBER
RESILIENCE
CENTRE

FOR THE **EAST MIDLANDS**