What is Cyber Essentials?

Cyber Essentials is a UK government-backed scheme designed to help businesses protect themselves against common cyber threats. There are two levels of assessment:

Cyber Essentials

Basic checks to ensure your organization meets five basic security controls. An assessor will verify the information provided.

Cyber Essentials plus

This certification builds on the basic requirements by including additional verification steps. This will involve a technical audit and vulnerability scans by a certified cybersecurity assessor.

Does my organization need cyber essentials?

When bidding for contracts, it's often a requirement to demonstrate they meet Cyber Essentials requirements, the contract will often specify if they require you to meet Cyber Essentials or Cyber Essentials Plus. Even if Cyber Essentials isn't a requirement, it will certainly go some way to helping you win the contract.

Are there any other advantages to obtaining Cyber Essentials Certification

Reassure customers that you are working to secure your IT against cyber-attack. Protect against your files getting lost, into the wrong hands, or scammers taking large payments from you. Attract new business with the certification to prove you have cyber security measures in place. You have a clear picture of your organization's cyber security level. Some businesses can save on their insurance by producing Cyber Essentials certification.

Can I implement Cyber Essentials myself?

Yes, if you wish to implement the Cyber Essentials requirements yourself you may self-assess your organization. Use this link to see pricing and download a self-assessment questionnaire.
https://iasme.co.uk/cyber-essentials/

What changes can I expect to see when Cyber Essentials is implemented?

From a user perspective, you can expect to see any unnecessary software applications to be removed, and the remaining software to be updated. Account lockdown, meaning administrative credentials will need to be entered to install software or make some changes. Increased password controls such as two-factor authentication, minimum password lengths and account lockout after several failed password attempts. Autorun for memory sticks and other removable media will be disabled. Various policies will be put in place. Behind-the-scenes firewall implementation, lockdown and updates. With Cyber Essentials Plus there will be more in-depth security scanning, checks, and corrective work on your PCs and servers. You may expect to provide information about your tablets and mobile phones, such as providing screenshots to prove they haven't been rooted or jailbroken, as well as showing the software has been updated and is in support. Any older devices may need to be replaced or decommissioned. If guests or employees use Wi-Fi for their personal devices, then a guest WIFI network will be created that is separated from your main network for this purpose.

What if I need to run an older non-compliant machine or software?

Sometimes this is possible by implementing suitable controls, such as keeping this device offline and separate from your main office network.

Do our mobile phones, tablets, including personally owned devices need to be included in Cyber Essentials?

Cyber essentials cover all devices that connect to the internet and contain or process data. If for example your device has access to your companies' emails, documents, or other systems then it will be in the scope of Cyber Essentials.

How long does Cyber Essentials Certification last, does it have to be renewed?

Certification lasts for 1 year and will need to be renewed for continual certification.

Will Cyber Essentials guarantee my system is fully protected and secure?

Cyber essentials is a basic level of security, it doesn't guarantee you are fully protected and secure. It covers five key controls: firewalls, secure configuration, user access control, malware protection, and patch management. These are essential for defending against common cyber threats but do not cover all aspects of cybersecurity. Cybersecurity also depends on the behavior of individuals within the organization. Phishing attacks, social engineering, and insider threats are examples where human error or malicious intent can bypass technical controls.

What are the costs of obtaining Cyber Essentials?

The costs really depend upon the scale of your I.T. system, how much work is required to bring your system to meet requirements, and what systems you already have in place to ensure your systems are kept up to standard. A gap analysis report can often help understand what work is required and what costs will be involved. Realistic prices **start** at around £700.00 for a very small system for Cyber Essentials. Cyber essentials Plus costs **start** at around £1800.00. Often a support plan will be required to ensure software/ firmware updates are in place. When looking at pricing ensure you understand what is covered i.e. initial gap analysis, everything you need to bring your system up to standard, required policies, and ongoing updates, check, security software and protection.