vivo comms

EBOOK

Cyber Essentials

A government-backed scheme to help you to protect your business from online threats and demonstrate a cyber security focused mindset to your customers.

Introduction

Cyber Essentials Accreditation & Certification

The UK Government believes that being Cyber Essentials accredited could prevent “around 80% of cyber-attacks” and is crucial in improving your cyber security. Our CyberGuard team can guide your business through the steps towards achieving your Cyber Essentials accreditation with the minimum of fuss, assisting you through the whole process and will also be on hand to help you with any questions you may have along the way.

What is Cyber Essentials?

Cyber Essentials is a government-backed scheme that provide a clear statement of the basic controls all businesses should implement to mitigate the risk from common internet-based threats, within the context of the Government’s 10 Steps to Cyber Security. Secondly, through the Assurance Framework it offers a mechanism for organisations to demonstrate to their customers, investors, insurers, and others that they have taken these essential precautions.

The Cyber Essential Framework defines a set of five key security controls which, when properly implemented, will better protect businesses from internet-based attacks.

Five Cyber Essentials key controls

- **Boundary firewalls and internet gateways:** Devices are configured to prevent unauthorised access from inside or outside your private network, to your data and systems, while allowing secure access to those people who you do wish to allow access.
- **Secure configuration:** Device and software settings are as secure as possible.
- **Access control:** Allow only authorised personnel to have access to accounts, with permissions that reflect their roles in the organisation.
- **Malware protection:** Virus and malware protection is installed and up-todate as a necessary step to prevent Malware from penetrating your systems.
- **Patch management:** All software and applications are licensed, supported, and up-to-date with necessary patches. Also remove all software from devices that are no longer supported.

Note: All cloud services are included in the scope of the assessment.

Cyber Essentials & Cyber Essentials Plus

The Cyber Essentials scheme offers two levels of certification

Cyber Essentials: A basic level of certification based on a completed selfassessment questionnaire which is then verified and awarded by CyberGuard.

Cyber Essentials Plus: A higher level of assurance whereby CyberGuard will test that the five key security controls are working in practice by simulating basic hacking and phishing attacks.

Cyber Essentials

Cyber Essentials Plus is a self-assessment service.

As a certification body, CyberGuard will carry out an independent review of the answers you provide to the self-assessment questionnaire and award the certificate if you meet all the criteria.

If you are ready to take your Cyber Essentials assessment but would prefer to have a CyberGuard Consultant present as you go through the questionnaire on the Self-Assessment Portal, then we can provide this service.

Cyber Essentials Plus

Cyber Essentials Plus is an audited service.

CyberGuard's consultants will determine if you are following the Cyber Essentials guidelines by checking parts of your network and running several scans. Some customers are comfortable that everything is in place, as required, however others feel that they need an assessment prior to the audit. CyberGuard can offer both an assessment and the actual audit.

Readiness and Audit

Cyber Essentials Readiness Assessment

If you are considering attaining Cyber Essentials Plus accreditation and want a pre-assessment evaluation to identify any areas where you might fail, then CyberGuard can conduct a Readiness Assessment which includes:

- Authenticated Internal Vulnerability and Newt scan
- Firewall review (Boundary and Endpoint)
- Anti-Virus review
- Group Policy review
- Discuss internal processes that relate to the assessment, for example, a process for issuing and tracking admin users, creating and deleting users
- A report advising on any areas where you need to make improvements, or changes, to pass the Cyber Essentials Plus audit.

Note: It is often likely that remediation work and process development will be required following on from the readiness assessment. This work would most likely generate additional charges from your IT Support provider. Remediation work is not undertaken by CyberGuard as part of the Readiness Assessment. The Readiness Assessment does not include the actual audit and certification.

Cyber Essentials Plus Audit

As a certification body, CyberGuard can conduct the audit and award the certificate if you meet all the criteria. One of our Cyber Assessors will link to you remotely to conduct an audit against the criteria specified for Cyber Essentials Plus.

Note:

- Should you fail, you only have 30 days to remediate / demonstrate that you are in line with the requirements.
- After 30 days, re-tests will be chargeable.
- Cyber Essentials Plus must be completed within 3 months of being certified with Cyber Essentials.
- If 3 months elapses, you have to start back at the beginning with Cyber Essentials.

WWW.VIVOCOMMS.CO.UK

02476 620 250

Vivo Telecommunications Ltd
Friars House
Manor House Drive
Coventry
CV1 2TE

contact@vivotelecommunications.co.uk

vivo comms

Networking & Connectivity

Unified Communications & Voice

Contact Centres

Mobile Solutions & IoT

IT, Cloud & Technology

Network Intelligence

Cyberguard