CYBER ESSENTIALS CERTIFICATIONS

WHAT IS CYBER ESSENTIALS?

The Cyber Essentials Scheme was developed and launched by the UK Government. Cyber Essentials offers you an easy to implement foundation level certification with a basic level of assurance which an organisation can attain following a verified self-assessment. Implementing this first step helps to prevent cyber-attacks, providing basic level security measures to protect your income, resources, clients and reputation. It designed for small businesses which need to start with foundational protection.

WHAT IS CYBER ESSENTIALS PLUS?

Cyber Essentials Plus is the higher of the two government backed certifications to demonstrate a baseline standard for information technology security. The Cyber Essentials Plus accreditation comprises remote and on-site vulnerability testing to assess whether the basic security controls have been successfully implemented and is, therefore, the more rigorous assessment.

WHY SHOULD CYBER ESSENTIALS BE A PRIORITY?

The Cyber Essentials and Cyber Essentials Plus certificates help prevent and minimise a cyber security breach. Security breaches of any size can result in damage an organisation's reputation with negative press and erode customer loyalties, threaten large deals and acquisitions in addition to the financial loss involved. The certification also demonstrates to your clients and business partners that you take data protection seriously and that you take care to have adequate protection for their information as well as your own.

The Cyber Essentials Plus certification is mandatory for government contracting and is a recognised symbol for safe businesses in the United Kingdom.

OUR CYBER ESSENTIALS PROCESSES

PGI is an official UK Cyber Essentials and Cyber Essentials Plus certifying body and is able to offer both levels of certification to an organisation based on their requirements.

- Both certifications contain a self assessment questionnaire which establishes whether adequate policy and processes are implemented and, identifies whether the implementation of these security controls and malware protection is of an appropriate standard. Where needed PGI will guide clients through this. We will also review your self-assessment and suggest practical, low cost and timely processes to improve. This is the only stage for Cyber Essentials Certification.

In addition to the above, Cyber Essentials Plus continues through the following stages:

- We will conduct an offsite external assessment to identify vulnerabilities within the scope of external threats. This assessment will include port scans an automated vulnerability assessment and web application scanning. If this assessment is failed a retest will be scheduled once the organisation has fixed the vulnerabilities.
- We will then require physical access to the devices while onsite for an internal workstation assessment to identify vulnerabilities in workstation configurations, gaps in malware protection, browser protection, patch management and access control. This includes a workstation vulnerability scan as well as browser and malware protection tests.
- An additional onsite internal mobile device test will be performed including similar assessments as those conducted on workstations mentioned above but with further focus on encryption and physical protection. Personal devices used for work are included in this, however, these devices will not be tested by the consultant during his visit to the organisation's offices in order to protect the confidentiality of employee's personal data.
- Our final report will be delivered using the standardised template provided by the accreditation body. At the end of the assessment, the customer will be awarded a certificate with PGI, Accreditation and Cyber Essentials logos. This will demonstrate competence in security, and illustrate that the organisation meets baseline security standards set by the government.

The Cyber Essentials Plus assessment will typically span a week, the certification will be received once the accreditation body has reviewed the application, but it may be delayed if there are large security issues within the organisation that need to be addressed.

Each certification lasts for 12 months, after which a complete retest will need to be conducted. This is a requirement by the governing body to ensure that all certified companies keep their systems and networks up to date.

Cascades 1 | 1190 Park Avenue | Aztec West | Bristol | BS32 4FP | UK
Tel: +44 (0) 207 887 2699 Email: clientservices@pgitl.com Visit: www.pgitl.com

CYBER ESSENTIALS PLUS