Pentest Limited - IT security and penetration services

Cyber Essentials Questionnaire

**Introduction**

The Cyber Essentials scheme is recommended for organisations looking for a base level Cyber security test where IT is a business enabler rather than a core deliverable. It is mainly applicable where IT systems are primarily based on Common-Off-The-Shelf (COTS) products rather than large, heavily customised, complex solutions.

The main objective of the Cyber Essentials assessment is to determine that your organisation has effectively implemented the controls required by the Scheme, in order to defend against the most common and unsophisticated forms of cyber-attack.

The completed questionnaire attests that you meet the [Requirements of the Cyber Essentials Scheme](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf), which must be approved by a **Board member or equivalent**, and will then be verified by a competent assessor from **Pentest Ltd** (the Certifying Body). Such verification may take a number of forms, and could include, for example, a telephone conference. The verification process will be at the discretion of Pentest Ltd.

**On completion of the questionnaire**

|  |
| --- |
| When you have completed the document you should email it to; |
| Jed Kafetz |
| 0800 231 5977  Jed.kafetz@pentest.co.uk |
|  |
|  |
|  |
| If you wish to send it securely please contact Jed for details.  **REMEMBER TO ENSURE IT HAS BEEN SIGNED BY A SENIOR MEMBER OF YOUR COMPANY.** |
|  |

**How to avoid delays & additional charges**

You may incur additional charges if details are not sufficiently supplied, answer the questions as fully as possible giving supporting comments, paragraphs from policies and screen shots where possible. As a rule of thumb if it takes longer to assess the submission than you spent preparing it, you may be charged.

**Organisation Identification**

Please provide details as follows:

|  |  |
| --- | --- |
| Organisation Name (legal entity): |  |
| Sector: |  |
| Parent Organisation name (if any): |  |
| Size of organisation micro, small, medium, large.  (See definition below) |  |
| No of employees |  |
| Point of Contact name:  Salutation (Mr, Mrs, Miss etc)  First  Surname |  |
| Job Title: |  |
| Email address: |  |
| Telephone Number: |  |
| Contact Name for invoice (if different) |  |
| Invoice email address (if different) |  |
| Main web address for company in scope: |  |
| Building Name/Number  Address 1  Address 2  Address 3  City  County  Postcode |  |
| If you have used an [ACE Practitioner](http://www.qgstandards.co.uk/accredited-practitioners/) please provide their contact details: |  |
| Certification Body: | **Pentest Ltd** |
| Do you wish to be **excluded** from the register of Cyber Essentials certified companies. Exclusion means customers will not be able to find your entry. If this is left blank you will be entered. |  |
| From time to time government departments and other interested bodies may wish to use your company for marketing Cyber Essentials. If you do not wish to be promoted in this way please enter **NO** in the box. If this is left blank you imply your consent. |  |

**SME Definition**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Company category** | **Employees** | **Turnover** | or | | **Balance sheet total** |
| Medium-sized | < 250 | ≤ € 50 m | | ≤ € 43 m | |
| Small | < 50 | ≤ € 10 m | | ≤ € 10 m | |
| Micro | < 10 | ≤ € 2 m | | ≤ € 2 m | |

**Business Scope**

Please identify the scope of the system(s) to be assessed under this questionnaire, including locations, network boundaries, management and ownership. Where possible, include IP addresses and/or ranges.

A system name should be provided that uniquely identifies the systems to be assessed, and which will be used on any certificate awarded. (Note: it is not permissible to provide the company name, unless all systems within the organisation are to be assessed):

|  |
| --- |
|  |

Boundary Firewalls and Internet Gateways

|  |  |  |  |
| --- | --- | --- | --- |
|  | Question | Answer | Comment |
| 1 | Have you installed Firewalls or similar devices at the boundaries of the networks in the Scope? | Always  Mostly  Sometimes  Rarely  Never |  |
| 2 | Have the default usernames/passwords on all boundary firewalls (or similar devices) been changed to a strong password | Always  Mostly  Sometimes  Rarely  Never |  |
| 3 | Have all open ports and services on each firewall (or similar device) been subject to justification and approval by an appropriately qualified and authorised business representative, and has this approval been properly documented? | Always  Mostly  Sometimes  Rarely  Never |  |
| 4 | Have all commonly attacked and vulnerable services (such as Server Message Block (SMB) NetBIOSm tftp, RPC, rlogin, rsh, rexec) been disabled or blocked by default at the boundary firewalls? | Always  Mostly  Sometimes  Rarely  Never |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Question | Answer | Comment |
| 5 | Confirm that there is a corporate policy requiring all firewall rules that are no longer required to be removed or disabled in a timely manner, and that this policy has been adhered to (meaning that there are currently no open ports or services that are not essential for the business)? | Policy exists and has been implemented  Policy exists but has not been implemented  Policy does not exist |  |
| 6 | Confirm that any remote administrative interface has been disabled on all firewall (or similar) devices? | Always  Mostly  Sometimes  Rarely  Never |  |
| 7 | Confirm that where there is no requirement for a system to have Internet access, a Default Deny policy is in effect and that it has been applied correctly, preventing the system from making connections to the Internet | Always  Mostly  Sometimes  Rarely  Never |  |

Please provide any additional evidence to support your assertions above:

**Secure Configuration**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Question | Answer | Comment |
| 8 | Have all unnecessary or default user accounts been deleted or disabled | Yes  No |  |
| 9 | Confirm that all accounts have passwords, and that any default passwords have been changed to strong passwords? | Always  Mostly  Sometimes  Rarely  Never |  |
| 10 | Has all unnecessary software, including OS utilities, services and applications, been removed or disabled | Always  Mostly  Sometimes  Rarely  Never |  |
| 11 | Has the Auto Run (or similar service) been disabled for all media types and network file shares? | Always  Mostly  Sometimes  Rarely  Never |  |
| 12 | Has a host based firewall been installed on all desktop PCs or laptops, and is this configured to block unapproved connections by default? | Installed and configured  Installed, but not configured  Not installed |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 13 | Is a standard build image used to configure new workstations, does this image include the policies and controls and software required to protect the workstation, and is the image kept up to date with corporate policies? | Yes  No |  |
| 14 | Do you have a backup policy in place, and are backups regularly taken to protect against threats such as ransomware? | Yes  No |  |
| 15 | Are security and event logs maintained on servers, workstations and laptops? | Yes  No |  |

Please provide any additional evidence to support your assertions above:

**Access Control**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Question | Answer | Comment |
| 16 | Are user account requests subject to proper justification, provisioning and an approvals process, and assigned to named individuals? | Yes  No |  |
| 17 | Are users required to authenticate with a unique username and strong password before being granted access to computers and applications? | Yes  No |  |
| 18 | Are accounts removed or disabled when no longer required? | Yes  No |  |
| 19 | Are elevated or special access privileges, such as system administrator accounts, restricted to a limited number of authorised individuals? | Yes  No |  |
| 20 | Are special access privileges documented and reviewed regularly (e.g. quarterly)? | Yes  No |  |
| 21 | Are all administrative accounts only permitted to perform administrator activity, with no Internet or external email permissions? | Yes  No |  |
| 22 | Does your password policy enforce changing administrator passwords at least every 60 days to a complex password? | Yes  No |  |

Please provide any additional evidence to support your assertions above:

**Malware Protection**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Question | Answer | Comment |
| 23 | Please confirm that malware protection software has been installed on at least all computers with an ability to connect outside of the network in Scope | Always  Mostly  Sometimes  Rarely  Never |  |
| 24 | Does corporate policy require all malware protection software to have all engine updates applied, and is this applied rigorously? | Yes  No |  |
| 25 | Have all anti malware signature files been kept up to date (through automatic updates or through centrally managed deployment)? | Yes  No |  |
| 26 | Has malware protection software been configured for on-access scanning, and does this include downloading or opening files, opening folders on removable or remote storage, and web page scanning? | Yes  No |  |
| 27 | Has malware protection software been configured to run regular (at least daily) scans? | Yes  No |  |
| 28 | Are users prevented from running executable code or programs form any media to which they also have write access?  Other than anti-virus software, are access control measures in place to prevent virus code modifying commonly run executable files | Always  Mostly  Sometimes  Rarely  Never |  |
| 29 | Are users prevented from accessing known malicious web sites by your malware protection software through a blacklisting function? | Yes  No |  |

Please provide any additional evidence to support your assertions above:

Patch Management

|  |  |  |  |
| --- | --- | --- | --- |
|  | Question | Answer | Comment |
| 30 | Is all software installed on computers and network devices in the Scope licensed and supported? | Always  Mostly  Sometimes  Rarely  Never |  |
| 31 | Are all Operating System security patches applied within 14 days of release? | Always  Mostly  Sometimes  Rarely  Never |  |
| 32 | Are all Application software security patches applied within 14 days of release? | Always  Mostly  Sometimes  Rarely  Never |  |
| 33 | Is all legacy or unsupported software isolated, disabled or removed from devices within the Scope? | Yes  No |  |
| 34 | Is a mobile working policy in force that requires mobile devices (including BYOD) to be kept up to date with vendor updates and app patches? | Yes  No |  |

Please provide any additional evidence to support your assertions above:

**Approval**

It is a requirement of the Scheme that a Board level (or equivalent) of the organisation has approved the information given. Please provide evidence of such approval:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | | When you have completed the document you should email it to; | | |  | | --- | |  | | Jed Kafetz | | 0800 231 5977  Jed.kafetz@pentest.co.uk | |  | | |  | |  | | If you wish to send it securely please contact Jed for details.  **REMEMBER TO ENSURE IT HAS BEEN SIGNED BY A SENIOR MEMBER OF YOUR COMPANY.** | | |  | |  | |  | |  | |  | |  | |
|  |
|  |
|  |
|  |
|  |
|  |