



Cyber Essentials - Requirements for IT Infrastructure 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.

This questionnaire provides evidence for both **Level 1 Cyber Essentials and Level 2 Cyber Essentials PLUS.**

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. When completing this questionnaire you must do it in conjunction with the **Cyber Essentials – requirements for IT Infrastructure 06/02/2017**

The completed questionnaire attests that you meet the [Requirements for IT infrastructure 06/02/17,](http://www.qgstandards.co.uk/wp-content/uploads/2017/07/Requirements-for-IT-Infrastructure-QG-14-696-1.2.pdf) which **must be approved by a Board member** or equivalent, and will then be verified by a competent assessor from Seric Systems 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 Seric Systems Ltd.

**On completion of the questionnaire**

|  |
| --- |
| Please return the completed document to: |
|  |
| Ross Monteith  0141 561 1161 |
| [ross.monteith@seric.co.uk](mailto:ross.monteith@seric.co.uk) |

If you wish to send it securely please contact Ross for details.

**REMEMBER TO ENSURE IT HAS BEEN SIGNED BY A SENIOR MEMBER OF YOUR ORGANISATION**

**Scope of Cyber Essentials**

The Scope is defined in the threats in scope document, available on the official scheme website at <https://www.ncsc.gov.uk/information/threats-scope-cyber-essentials-scheme>

You will be required to identify the actual scope of the system(s) to be evaluated as part of this questionnaire.

**How to avoid delays & additional charges**

You may incur delays or additional charges if details are not sufficiently supplied. Please answer each question as fully as possible, with 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.

**Please note: Copies of your organisational policies and procedures may be provided as evidence, please include a reference to page or paragraph numbers within the response below.**

**Organisation Identification**

Please provide details as follows:

|  |  |
| --- | --- |
| Date of Application |  |
| 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 |  |
| Certification Body: | Seric Systems Ltd. |
| If you have used an [ACE Practitioner](http://www.qgstandards.co.uk/accredited-practitioners/) please provide their contact details: |  |
| Do you wish to be **included** in the register of Cyber Essentials certified companies. Inclusion means customers will 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/research purpose. If you do not wish to be promoted/utilised in this way please enter **NO** in the box. If this is left blank you imply your consent. |  |
| Where did you hear about Cyber Essentials? |  |
| If this is a recertification – please enter your Certificate Number |  |

**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 | |

As a Cyber Essentials scheme Applicant, you must ensure that your organisation meets all the requirements. You are also required to supply various forms of evidence before Seric can award certification at the level you seek. Please use **screen grabs** and **insert policy notes** where possible.

**Let’s get started;**

**Whilst completing this questionnaire please use the document, ‘Requirements for IT infrastructure’ published by QG (6th February 2017). We have cross referenced each clause and question so you can see clearly the intent of the question you are answering at the time.**

1. Establish the **boundary of scope** for your organisation, and determine **what is in scope within this boundary**. (including locations, network boundaries, management and ownership. Where possible, include IP addresses and/or ranges.)
2. Ensure your password policy is in place and meets the password based-authentication requirements, as this is used in three of the five control themes.
3. Review each of the five **technical control themes** and the **controls they embody as requirements**.
4. Take steps as necessary to **ensure that your organisation meets every requirement**, throughout the scope you have determined. If you can’t, highlight any **compensating controls** you have put in place to mitigate the risk.
5. **Business Scope**

A network 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):

|  |
| --- |
| Please include:   * The name of your in-scope network. * Whether the network is single or multiple sites (if multiple, how are they connected)? * If any systems are out-of-scope, how are they separated to prevent impacting data within the in-scope network? * If any, which Cloud services are used (e.g. Dropbox, Office 365, Google Drive) * For each Cloud Service please provide a link or supplemental documentation detailing the provider’s security controls and certifications.   Remember: You may place SaaS file-storage solutions such as Dropbox or Google Drive out-of-scope (where you are not responsible for patching the operating systems on these products). If the data on these systems is to be protected by Cyber Essentials, then each of your endpoints that can access data on the SaaS solution must be in scope. |

1. **Password-based authentication**

The Applicant must make good use of the technical controls available to it on password-protected systems. As much as is reasonably practicable, technical controls and policies must shift the burden away from individual users and reduce reliance on them knowing and using good practices.

Users are still expected to pick sensible passwords.

For password-based authentication in **Internet-facing** services the Applicant must:

* protect against brute-force password guessing, by using at least one of the following methods:
  + lock accounts after no more than 10 unsuccessful attempts
  + limit the number of guesses allowed in a specified time period to no more than 10 guesses within 5 minutes
* set a minimum password length of at least 8 characters
* not set a maximum password length
* change passwords promptly when the Applicant knows or suspects they have been compromised
* authenticate users before granting access to applications and devices, using unique credentials
* have a password policy that tells users:
  + how to avoid choosing obvious passwords (such as those based on easily-discoverable information like the name of a favourite pet)
  + not to choose common passwords — this could be implemented by technical means, using a password blacklist
  + not to use the same password anywhere else, at work or at home
  + where and how they may record passwords to store and retrieve them securely — for example, in a sealed envelope in a secure cupboard
  + if they may use password management software — if so, which software and how
  + which passwords they really must memorise and not record anywhere

**The Applicant is not required to:**

* enforce regular password expiry for any account
* enforce password complexity requirements

|  |  |  |
| --- | --- | --- |
| **Clause** | **Requirement** | **Evidence/Narrative/Compensating control** |
| 2.1 | If applicable describe the technical controls used to enforce the password policy. | Remember to include the controls against password brute-force (guessing) attacks. |
| 2.2 | If applicable, describe paper based controls used to enforce the password policy. |  |
| 2.3 | Confirm that you have implemented a password policy which meets the requirements of the Password-based authentication requirements (above) | Only required for internet-facing systems. |

1. Firewalls

Objective

Ensure that only safe and necessary network services can be accessed from the Internet.

**Applies to:** boundary firewalls; desktop computers; laptop computers; routers; servers.

|  |  |  |
| --- | --- | --- |
| **Clause** | **Requirement** | **Evidence/Narrative/Compensating control** |
| 3.1 | Describe how your firewalls are placed in your network | If you have a boundary firewall device, describe it here. Also describe any other firewalls on your network, e.g. between departments. |
| 3.2 | Tick all that apply | (delete as appropriate)  **Office Environment**   1. All desktop/laptops have a properly configured host-based firewall 2. Some desktop/laptops have a properly configured host-based firewall 3. No desktop/laptops have a properly configured host-based firewall   If b) or c) is chosen, you will not pass this question if you do not have a firewall at the boundary of the network.  **Untrusted Environment (not work network)**   1. desktop/laptops have a properly configured host-based firewall when connected to untrusted networks such as public wi-fi hotspots. (this point is mandatory) 2. desktop/laptops **do not** have a properly configured host-based firewall when connected to untrusted networks such as public wi-fi hotspots.   You will not pass this question if laptops/desktops do not have a properly configured host-based firewall when connected to untrusted networks such as public wi-fi hotspots. |
| 3.3 | All default administrative passwords must be changed to an alternative password that is difficult to guess in line with your password policy, is this the case? | This question only refers to passwords on boundary firewall and network protection devices. Please include any that are accessible from your internal network. Confirm that all manufacturer default passwords have been changed. |
| 3.4 | How is each firewall administrative interface protected from direct access via the internet? | Controls may include:   * Multi Factor Authentication * Denying access to the administrative interface, from the internet (can only be accessed from your internal network). * Restricting access to trusted IP addresses, through Access Control Lists. |
| 3.5 | All unauthenticated inbound connections must be blocked by default (i.e. not allowed until approved), is this the case? | Please answer “Yes” or “No” and describe how this is achieved. |
| 3.6 | If inbound firewall rules are configured, they must be approved and documented, is this the case? | Describe any processes for introducing new firewall rules, such as approval forms, updating a spreadsheet or change control. Also include a note of any approvers (job title or role). |
| 3.7 | Are firewall rules no longer required removed quickly? | Describe any processes or mechanisms that ensure redundant firewall rules are promptly removed. This may be supplemented with regular reviews of the firewall rule base. |

Please provide any additional evidence to support your assertions for section 3

1. **Secure Configuration**

Objective

Ensure that computers and network devices are properly configured to:

* reduce the level of inherent vulnerabilities
* provide only the services required to fulfil their role

**Applies to**: email, web, and application servers; desktop computers; laptop computers; tablets; mobile phones; firewalls; routers.

|  |  |  |
| --- | --- | --- |
|  | **Requirements** | **Evidence/Narrative/Compensating control** |
| 4.1 | Do you have a ‘documented’ password policy that contains the requirements of section 2? | The password policy must extend to any internet facing services. Please provide the name of the password policy and paste the relevant text here. |
| 4.2 | All unnecessary user accounts (e.g. guest accounts and unnecessary administrative accounts) must be removed or disabled on all devices. Is this the case? | When was this carried out or last-checked, and by whom? |
| 4.3 | All default or guessable passwords for user accounts on all devices must be changed to a non-obvious password. | Confirm that any vendor default passwords have been changed and that you do not use a ‘default’ password across multiple user accounts. |
| 4.4 | **Unnecessary** software (including applications, system utilities and network services) must be removed or disabled, is this the case? | The purpose of this, is to reduce the attack surface of your devices by removing functionality that is not required. Remember to disable any non-required network services or functionality in the OS. |
| **4.5** | In order to prevent untrusted programs running automatically, (**including those from the internet**) have you disabled any feature that would allow the such files to auto-run or, at least, is user authorisation required before file execution?  Describe how this has been achieved. | **Remember to include how files accessed via web browsers are handled. This question isn’t limited to auto-running of files on CD / USB media.**    Investigate whether the malware protection software helps to prevent suspicious program behaviour and that Operating System controls to prevent untrusted files running have been activated.  Smart Screen Filter, Software Restriction Policies may be one such control for windows based systems. Only allowing trusted/signed programs may be such a control that can be used in Linux / Macintosh environments.  For example, the following Microsoft page provides a variety of (safe) sample attacks that should not run without informing of the possible consequences:  <https://demo.smartscreen.msft.net/> |
| 4.6 | How do you control internet-based access to any areas containing commercially, personally sensitive data or any data which is critical to the running of the organisation ? | This describes access from the internet, to information held on your company servers (web, email and application) or laptop / desktop computers. Remember that the password requirements for internet facing services will apply here. |

Please provide any additional evidence to support your assertions for section 4:

1. **User Access Control**

Objective

Ensure user accounts:

* are assigned to authorised individuals only
* provide access to only those applications, computers and networks actually required for the user to perform their role

**Applies to:** email, web and application servers; desktop computers; laptop computers; tablets; mobile phones.

|  |  |  |
| --- | --- | --- |
|  | **Requirements** | **Evidence/Narrative** |
| 5.1 | It is a requirement that you have identified all locations where sensitive and businesses critical information is stored digitally. (email, web and application servers, data shares, end user devices etc) Has this been done? | Describe how you have documented this (for example, use of spreadsheets, Information Asset Register etc) |
|  | For the locations identified above, answer the following questions |  |
| 5.2 | Does the organisation have a user account creation and approval process? | How is this achieved, e.g. linked to HR or payroll processes? |
| 5.3 | Does the organisation authenticate users before granting access in compliance with the defined password policy? | This requirement is for password-based authentication in Internet-facing services (however we recommend your password policy cover all types of accounts) |
| 5.4 | Has the organisation removed or disabled user accounts when no longer required? | Describe how this is triggered (e.g. linked to HR processes) and if any additional periodic checks are carried out. |
| 5.5 | Where feasible, has the organisation implemented two factor authentication? | **We are only concerned with the “feasible” implementation of two factor authentication and understand that roll-out can be costly and time consuming – especially for larger organisations.**  As well as access to on-premise accounts via the internet, Cloud accounts must also be considered such as those mentioned here:  <https://www.ncsc.gov.uk/guidance/password-guidance-summary-how-protect-against-password-guessing-attacks>  Identify areas where Multi Factor Authentication (sometimes referred to two-factor authentication, 2FA or two-step verification) has been implemented.  Please also identify areas where this could have been implemented but hasn’t – and give justification for this.  Describe any any roll-out plans you have, along with timescales. |
| 5.6 | Are administrative accounts used to perform administrative activities ONLY? (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks). | **It is very important that you ensure administrators – even administrators of local machines - do not browse untrusted websites or open email attachments otherwise any executed malware could take full control of the device.**  One approach is for users to be standard users for day-to-day use. This way, if a user contracts malware, it will not be able to change security settings, enable / disable services etc, without alerting the user to log-in as an administrator first.  We understand that some applications require users to have administrator privileges in order to function correctly.  These are generally the exception rather than the rule and you must identify if running such programs with Administrator privileges can be achieved and not allow users to change system settings should they open a malicious file  If you must browse the web, or use email, using Administrator privileges, then this questionnaire **should not be submitted** without very good alternative technical controls (such as only allowing trusted whitelisted websites, attachment blocking, application whitelisting or sandboxing – defined in 6.2 and 6.3) |
| 5.7 | Does the organisation remove or disable special access privileges when no longer required? | What is the process to ensure this is done quickly?  Regular reviews are a good additional step to discover any accounts that have been missed, but there must be a mechanism to trigger prompt removal of special privileges between reviews. |

Please provide any additional evidence to support your assertions for section 5.

1. **Malware Protection**

Objective

Restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data.

**Applies to:** desktop computers; laptop computers; tablets; mobile phones.

|  |  |  |
| --- | --- | --- |
| The organisation must implement a malware protection mechanism on all devices that are in scope. For each such device, the organisation must use **at least one** of the three mechanisms listed below: | | |
| 6.1 | Anti-Malware Software | Evidence / Narrative |
| 6.1.1 | How is the daily update of the anti-malware software (and all associated malware signature files) managed? | Checks for virus signature / definition updates must be at least daily. |
| 6.1.2 | Is the software configured to scan files automatically upon access (including when downloading and opening files, and accessing files on a network folder)? | Please only answer “yes” to this question if you are confident that your anti-malware software scans files on access.  You may wish to try downloading the EICAR anti-virus test files at <http://www.eicar.org/85-0-Download.html> to help confirm this. The files should be automatically detected and blocked by your anti malware software.  Note: The running of full scheduled scans is not essential, but may be a useful additional control. |
| 6.1.3 | Are web pages scanned automatically upon access either by the web browser itself, the anti-malware software or by a third party service? | We accept evidence of web anti-malware functionality within anti-malware software, web browsers or web gateway services or devices. |
| 6.1.4 | Does the software prevent connections to malicious websites by means of blacklisting? | We accept evidence that anti-malware software, web browsers, web gateway services or devices have this function enabled. |
| 6.2 | **Application whitelisting** | Evidence / Narrative |
| 6.2.1 | Are only approved applications, restricted by code signing, allowed to execute on devices? | This **must** be the case if application whitelisting is your only defensive mechanism |
| 6.2.2 | Does the organisation actively approve such applications before deploying them to devices? | Users **must** do this if application whitelisting is your only defensive mechanism |
| 6.2.3 | Does the organisation maintain a current list of approved applications? | Users **must** do this if application whitelisting is your only defensive mechanism |
| 6.2.4 | Are users able to install any application that is unsigned or has an invalid signature? | Users **must not** be able to do this if application whitelisting is your only defensive mechanism |
|  | **Application sandboxing** | Evidence / Narrative |
| 6.3 | Is all code of unknown origin run within a 'sandbox' that prevents access to other resources unless permission is granted by the user? (including other sandboxed applications, data stores, such as those holding documents and photos, sensitive peripherals, such as the camera, microphone and GPS or local network access | This **must** be the case is Application Sandboxing is your only defensive mechanism. |

Please provide any additional evidence to support your section 6

1. **Patch Management**

Objective

Ensure that devices and software are not vulnerable to known security issues for which fixes are available.

**Applies to:** web, email and application servers; desktop computers; laptop computers; tablets; mobile phones; firewalls; routers.

|  |  |  |
| --- | --- | --- |
|  | Statement | Evidence/Narrative |
| 7.1 | Is all software licensed and supported? | If any software is unsupported (i.e. no security updates are received), please say what the application is, if it is common off-the-shelf software and why it has not been upgraded to a supported version. |
| 7.2 | Is all software removed from devices in scope when no longer supported? |  |
| 7.3 | Is software patched within 14 days of an update being released, where the patch fixes a vulnerability with a severity that the product vendor describes as 'critical' or 'high risk' | **For the purposes of the Cyber Essentials scheme, 'critical' or 'high risk' vulnerabilities are those with the following values:**   * **Attack Vector: network only** * **Attack Complexity: low only** * **Privileges Required: none only** * **User Interaction: none only** * **Exploit Code maturity: functional or high** * **Report Confidence: confirmed or high**   The above conditions should be helpful for those companies with a high number of computers and only have time to apply the most relevant patches within 14 days.  Many smaller companies will generally patch all software regardless of severity. |
|  |  |  |

Please provide any additional evidence to support your assertions above:

1. **Approval**

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

Signature

Name

Position

Date