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, which **must be approved by a Board member** or equivalent, and will then be verified by a competent assessor from Securious (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 Securious.

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 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:

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:	Securious
If you have used an ACE Practitioner 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?	

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 Securious 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 06/02/17**' 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.

1. 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):

2. 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

For password-based authentication in Internet-facing and non-internet facing services the Applicant must:

- 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.	
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)	

3. Firewalls

Objective

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

Clause	Requirement	Evidence/Narrative/Compensating control
3.1	Describe how your firewalls are placed in your network	
3.2	Tick all that apply	Office Environment ○ All desktop/laptops have a properly configured host-based firewall ○ Some desktop/laptops have a properly configured host-based firewall ○ No desktop/laptops have a properly configured host-based firewall Untrusted Environment ○ desktop/laptops have a properly configured host-based firewall when connected to untrusted networks such as public wi-fi hotspots. (this point is mandatory)
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?	
3.4	How is each firewall administrative interface protected from direct access via the internet?	
3.5	All unauthenticated inbound connections must be blocked by default, is this the case?	
3.6	If inbound firewall rules are configured, they must be approved and documented, is this the case?	
3.7	Are firewall rules no longer required removed quickly?	

Please provide any additional evidence to support your assertions above:

4. 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

	Requirements	Evidence/Narrative/Compensating control
4.1	Do you have a 'documented' password policy that contains the requirements of section 2?	
4.2	All unnecessary user accounts (eg guest accounts and unnecessary administrative accounts) must be removed or disabled on all devices. Is this the case?	
4.3	All default or guessable passwords for user accounts on all devices must be changed to an alternative password in line with your password policy. Is this the case?	
4.4	**Unnecessary** software (including applications, system utilities and network services) must be removed or disabled, is this the case?	
4.5	In order to prevent untrusted programs running automatically, (including those from the internet) either the auto-run feature must be disabled or user authorisation must be actioned before file execution. Describe how this has been achieved.	
4.6	How is internet-based access controlled to any areas containing commercially, personally sensitive data or any data which is critical to the running of the organisation ?	

Please provide any additional evidence to support your assertions above:

5. 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

	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?	
	For the locations identified above answer the following questions	
5.2	Does the organisation have a user account creation and approval process?	
5.3	Does the organisation authenticate users before granting access in compliance with the defined password policy?	
5.4	Has the organisation removed or disabled user accounts when no longer required?	
5.5	Where available, has the organisation implemented two factor authentication?	
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).	
5.7	Does the organisation remove or disable special access privileges when no longer required?	

Please provide any additional evidence to support your assertions above:

6. Malware Protection

Objective

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

	Requirements	Evidence/Narrative
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**	
6.1.1	How is the daily update of the anti-malware software (and all associated malware signature files) managed?	
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)?	
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?	
6.1.4	Does the software prevent connections to malicious websites by means of blacklisting?	
6.2	**Application whitelisting**	
6.2.1	Are only approved applications, restricted by code signing, allowed to execute on devices?	
6.2.2	Does the organisation actively approve such applications before deploying them to devices?	
6.2.3	Does the organisation maintain a current list of approved applications?	
6.2.4	Are users able to install any application that is unsigned or has an invalid signature?	

6.3	**Application sandboxing**	
6.3.1	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	

Please provide any additional evidence to support your assertions above:

7. Patch Management

Objective

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

This applies to operating systems and application software on web, ……..

	Statement	Evidence/Narrative
7.1	Is all software licensed and supported?	
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'	

Please provide any additional evidence to support your assertions above:

8. 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