CYBER ESSENTIALS QUESTIONNAIRE

Introduction

The Cyber Essentials scheme is recommended for organisations looking for guidance on fundamental cyber security measures to protect them. It is applicable where IT systems are based on common off-the-shelf products rather than large, bespoke or complex solutions. Implementing Cyber Essentials guidance protects against the most common and unsophisticated forms of cyber-attack.

This questionnaire allows you to provide evidence for both Cyber Essentials (Level 1) and Cyber Essentials Plus (Level 2) assessments. The main objective of the Cyber Essentials assessment is to determine that your organisation has effectively implemented the controls required by the scheme.

The completed questionnaire attests that you meet the Requirements for IT infrastructure, which **must be approved by a Board member** or equivalent.

Once completed, and on payment of the appropriate fee, we will submit your application to our Certification Body for verification. Such verification may take several forms, and could include, for example, a telephone conference. The verification process will be at the discretion of the Certification Body.

For help with Cyber Essentials applications the Companion Guide to Cyber Essentials Questionnaire provides:

- Detailed guidance for each of the 30 questions
- Help with defining the Scope of the assessment
- 2 x FREE half-hour telephone consultations with an Accredited Cyber Essentials Practitioner
- An example Mobile Working Policy template

How to avoid delays & additional charges

You may incur additional charges from the Certification Body if details are not sufficiently supplied. Answer the questions as fully as possible giving supporting comments, paragraphs from policies and screen shots where possible.

Please ask about our Questionnaire Check service to ensure that your application is successful first time.

CYBER ESSENTIALS
QUESTIONNAIRE

Organisation Identification

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:	
Contact name:	
Job Title:	
Email address:	
Telephone Number:	
Contact Name for invoice (if different):	
Invoice email address (if different):	
Main web address for company in Scope:	
Company Address:	
Do you wish to be **included** in the register of Cyber Essentials certified companies? Inclusion means customers will be able to find your entry?	
Government departments and other interested bodies may wish to use your company for marketing/research purposes. Do you consent for your data to be used in this way?	
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

Further Guidance

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 the Certification Body can award certification at the level you seek. Please use **screen grabs** and insert **policy notes** where possible.

1. Establish the **boundary of scope** for your organisation, and determine **what is in Scope within this boundary**. Include locations, network boundaries, management and ownership of devices. Where possible, include IP addresses and/or ranges.

2. Review each of the six **technical control themes and the controls they embody as requirements**.

3. 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.

4. Your questionnaire answers contain extremely sensitive information. When submitting your application, please ensure that your questionnaire is **always** encrypted.

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:

- Number of sites in Scope
- How you ensure that any out-of-scope systems cannot influence the security of the data in Scope
- What Cloud Services are used (Dropbox, Office 365, Google Drive)
- A URL (or send supplemental documentation) that shows each cloud provider's security processes and certifications

Remember: though you may count SaaS file-storage solutions such as Dropbox or Google Drive as out-of-scope (i.e. 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 every endpoint that can access the data on that SaaS solution must be in Scope.

Control 1 - Password-based authentication

Password-based authentication must be used wherever it is necessary to access data and devices in Scope. This includes workstations, servers, mobile devices, and cloud-based services.

For password-based authentication in **Internet-facing** services you 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 period to no more than 10 guesses within 5 minutes
  - implement two-factor or multi-factor authentication

For password-based authentication in **Internet-facing and non-internet facing services** you must:

- set a minimum password length of at least 8 characters
- not set a maximum password length
- change passwords promptly when a compromise has occurred or is suspected
- 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

You are *not* required to:

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

#	Requirement	Evidence/Narrative
1	If applicable, what technical controls are used to enforce password policy?	
2	If applicable, what paper-based controls are used to enforce *Password Policy*?	
3	Confirm that you have implemented a *Password Policy* which meets the password-based authentication requirements (above)	Please give the name of the password policy and paste the relevant lines into this box.

Additional Evidence

Please provide any additional evidence to support your assertions for Control 1:

Control 2 - Firewalls

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

Applies to: boundary firewalls; desktops; laptops; routers; servers.

#	Requirement	Evidence/Narrative
4	How are boundary firewalls placed in your network?	
5	How are host-based firewalls configured in your network?	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 (Outside Scope 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.
6	Have default administrative passwords on boundary devices been changed to a password that is difficult to guess in line with your *Password Policy*?	Remember, this includes administrative interfaces accessed from the Local Area Network
7	How is each firewall administrative interface protected from direct access via the Internet?	Necessary controls could include: • Two Factor Authentication (Two step verification) • Disabling the remote administrative interface • Only allow trusted IP addresses to administer the device
8	Have all unauthenticated inbound connections been disabled or blocked by default at the boundary firewalls?	Please answer "Yes" or "No" Who is responsible for allowing connections (role)?
9	Have all inbound firewall rules been subject to justification and approval by an authorised business representative? Has this approval been properly documented?	Describe how this is achieved (such as filling out approval forms or updating a spreadsheet, for example)
10	What is the process for requiring all firewall rules that are no longer required to be removed quickly?	

Additional Evidence

Please provide any additional evidence to support your assertions for Control 2:

Control 3 - Secure Configuration

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.

#	Requirement	Evidence/Narrative
11	Have all unnecessary user accounts (e.g. guest accounts and unnecessary administrative accounts) been deleted or disabled?	When was this done and by whom?
12	Have all default or guessable passwords for user accounts on all devices and services been changed in line with your *Password Policy*?	When is this done and by whom?
13	Has all unnecessary software, including applications, system utilities and network services, been removed or disabled?	Don't forget to look at the network services used by each device and disable those that aren't required.
14	To prevent untrusted programs running automatically, the AutoPlay feature must be disabled. How has this been achieved?	
15	To prevent untrusted programs running automatically user authorisation must be actioned before file execution. How has this been achieved?	Investigate whether the malware protection software helps to solve this and that operating system controls to help prevent untrusted files running have been activated. To test, the following untrusted file should not run without informing of the possible consequences. https://demo.smartscreen.msft.net/download/unknown/freevideo.exe
16	How do you control internet-based access to any areas containing commercially or personally sensitive data?	This applies to servers (web, email and application) and laptop / desktop computers accessed via the web to access such information. Remember that the password requirements for internet facing services will apply here.

Additional Evidence

Please provide any additional evidence to support your assertions for Control 3:

Control 4 - User Access Control

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.

#	Requirement	Evidence/Narrative
17	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 (Information Asset Register etc)
	For the locations identified above, answer the following questions:	
18	Does the organisation have a user account creation and approval process?	
19	Does the organisation authenticate users before granting access in compliance with the defined *Password Policy*?	
20	Are accounts removed or disabled when no longer required?	
21	Where available, has the organisation implemented Multi Factor Authentication?	Cloud accounts must also be considered such as those mentioned here: https://ncsc.gov.uk/guidance/password-guidance-summary-how-protect-against-password-guessing-attacks Please also identify areas where this could have been implemented but hasn't – please state why.
22	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 the web or open attachments. The questionnaire should **not be submitted** without very good alternative technical controls if this is the case (such as only allowing whitelisted websites, attachment blocking, application whitelisting or sandboxing – defined in Control 5 – Malware Protection)
23	Does the organisation remove or disable special access privileges when no longer required?	

Additional Evidence

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

Control 5 - Malware Protection

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

The organisation must implement a malware protection mechanism on all devices that are in Scope.

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

Option A – Anti-Malware Software

#	Requirement	Evidence/Narrative
24	How is the daily update of the anti-malware software (and all associated malware signature files) managed?	
25	Is the software configured to scan files automatically upon access (including when downloading and opening files, and accessing files on a network folder)?	
26	Are web pages scanned automatically upon access either by the web browser itself, the anti-malware software or by a third-party service?	
27	Does the software prevent connections to malicious websites by means of blacklisting?	

As Anti-Malware Software is considered a fundamental layer in your Cyber Security defences, Control 5 is most easily satisfied by answering the previous 4 questions. However, in certain circumstances, additional controls can be used to satisfy Control 5. These are known as Application Whitelisting and Application Sandboxing.

If you are familiar with these approaches then you can answer either one or other of the following two sets of questions as an alternative to Anti-Malware Software.

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

Option B – Application Whitelisting

#	Requirement	Evidence/Narrative
24	Are only approved applications, restricted by code signing, allowed to execute on devices?	
25	Does the organisation actively approve such applications before deploying them to devices?	
26	Does the organisation maintain a current list of approved applications?	
27	Are users able to install any application that is unsigned or has an invalid signature?	Users must not be able to do this.

Option C – Application Sandboxing

#	Requirement	Evidence/Narrative
24	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)?	

Additional Evidence

Please provide any additional evidence to support your assertions for Control 5:

Control 6 - Patch Management

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

#	Statement	Evidence/Narrative
28	Is all software licensed and supported?	
29	Is all software removed from devices in Scope when no longer supported?	
30	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'?	

Additional Evidence

Please provide any additional evidence to support your assertions for Control 6:

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:	Date:
Name:	Position: