Cyber Essentials Application Form

Please complete this form using Microsoft Word or a compatible word processing programme, returning by email to enquiries@centreforassessment.co.uk. Alternatively, please complete in BLACK ink and CAPITALS and post to:

Centre for Assessment Ltd
Lee House
90 Great Bridgewater Street
Manchester
M1 5JW

If you require any assistance in completing this application, please do not hesitate to contact us on **0161 237 4080**

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, 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, QG BIS 49 696-1.2. This must be approved and signed by a Senior Manager with the approved authorisation level within the organisation. By signing and submitting the application form the organisation is agreeing to the terms and conditions of the assessment and agrees that the information provided in the questionnaire is correct and all sections have been completed.

The questionnaire will then be verified by a competent assessor appointed by Centre for Assessment Ltd (the Certifying Body). Such verification may take several forms, and could include, for example, a telephone conference. The verification process will be at the discretion of Centre for Assessment Ltd and their appointed assessors.

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 ensure that this questionnaire is completed in full and all questions are answered in full

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 name and Surname	
Job Title:	
Email address:	
Telephone Number:	
Main web address for company in scope:	
Building Name/Number Address City County Postcode	
Certification Body:	ID Cyber Solutions
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.

Yes ☐ No ☐

From time to time government departments and other interested bodies may wish to use your company for marketing/research purpose. Do you wish to be promoted/utilised in this way?

Yes ☐ No ☐

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 ID Cyber Solutions 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, QG BIS 49 696-1.2."

Please answer each question, adding as much detail as possible in the Comments/Evidence box. If you do not feel that you can fulfil the criteria of a question, please highlight any compensating controls which you have in place to mitigate the risk.

Please ensure that you complete all questions in all sections and provide all the evidence required. Yes/NO answers are not permitted

1. Business Scope

The business scope should outline the IT systems which you use to run your organisation.

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):

As a guideline, refer to the list below:

1. List all organisation sites/offices, which are in included in the business scope.

2. How many machines are on your network (laptops, desktops)?

3. What Operating Systems are installed on your machines?

4. List any servers within the organisation and what purpose they serve.

5. List any other network devices, such as boundary firewalls, routers, etc.

6. List any Cloud Services used within the organisation, such as Office 356, Dropbox, Google Drive.

7. If applicable, how is remote access managed to your organization (for example, by VPN, etc.).

8. Does your organisation use any third-party IT management service?

2. Password-based Authentication

The organization must make good use of available technical controls on password-protected systems and must maintain a written password policy. While users are still expected to pick sensible passwords, technical controls and policies must shift the burden away from individual users and reduce reliance on them knowing and using good practices.

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

- set a minimum password length of at least 8 characters
- not set a maximum password length
- change passwords promptly when the user knows or suspects they have been compromised

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 organisation is not required to:

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

Clause	Question	Comments/Evidence
2.1	Do you have a written password policy which meets the requirements laid out in Section 2 above?	
2.2	Describe the technical controls used to enforce your password policy (for example, to enforce minimum password length).	
2.3	For internet-facing services what method do you use to protect against brute-force password guessing (as described in section 2 above)?	

3. Firewalls

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

Every device must be protected by a correctly configured firewall. Please complete the options below which apply to you.

- Option 1 - We have at least one network-based firewall (for example, we have a router with a built-in firewall, or we have a dedicated firewall module)
- Option 2 - Our devices use host-based firewalls (for example, our anti-virus software includes a host-based firewall, or we use the built in Windows firewall)

Please choose and complete only the option(s) below which you use in your organization.

Option 1 – Network-based Firewall

Clause	Question	Comments/Evidence
3.1.1	Is the administrative interface of the firewall; a) password protected using a non-default, strong password, or b) disabled entirely?	
3.1.2	If enabled, how is the firewall's administrator interface protected from direct access from the internet (for example, is access limited to certain trusted IP addresses, or is two-factor authentication enabled)?	
3.1.3	All unauthenticated inbound connections must be blocked by default. Is this the case?	
3.1.4	If any inbound connections are permitted, the relevant firewall rules must be approved and documented. If this is the case, what is the approval and documentation process?	
3.1.5	If any inbound firewall rules are configured, these must be removed quickly once they are no longer required. If this is the case, how is this achieved?	

Option 2 – Host-based Firewall

Clause	Question	Comments/Evidence
3.2.1	All unauthenticated inbound connections must be blocked by default. Is this the case?	
3.2.2	If any inbound connections are permitted, the relevant firewall rules must be approved and documented. If this is the case, what is the approval and documentation process?	
3.2.3	If any inbound firewall rules are configured, these must be removed quickly once they are no longer required. If this is the case, how is this achieved?	

Clause	Question	Comments/Evidence
3.3	When connecting to untrusted networks (for example, public Wi-Fi hotspots) all devices must have a properly configured host-based firewall. If this is the case, how is this achieved?	

Please provide a Screenshot of Firewall shows that SMB/NetBIOS ports are being actively blocked

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**

Clause	Question	Comments/Evidence
4.1	All unnecessary user accounts (e.g. guest accounts and unnecessary administrative accounts) must be removed or disabled on all devices. Is this the case?	
4.2	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?	
4.3	**Unnecessary** software (including applications, system utilities, and network services) must be removed or disabled, is this the case?	
4.4	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 that 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.**

Clause	Question	Comments/Evidence
5.1	Does the organisation have a user account creation and approval process?	
5.2	Does your organization require users to log in before being granted access to applications or devices (In compliance with your defined password policy)?	
5.3	To prevent unnecessary exposure, are users granted only as much access to applications or devices as they need to perform their job roles?	
5.4	Has the organisation removed or disabled user accounts when no longer required (For example, when someone leaves the organization or changes their job role)?	
5.5	Where feasible, has the organisation implemented two factor authentications for accessing applications and/or devices?	
5.6	Are administrator accounts restricted to a limited number of authorised individuals?	
5.7	Administrative accounts must be used only to perform administrative activities. This means no day-to-day activities, such as emailing or web browsing, which may expose administrative accounts to avoidable risks. Is this the case?	
5.8	Does the organisation remove or disable access to administrative accounts when the user no longer requires it (for example, when a member of staff leaves the organization or changes their job role)?	

Please provide a Screenshot of typical client PC showing the local admin account

6. Malware Protection

Objective: 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. For each such device, the organisation must use **at least one** of the three mechanisms listed below:

- Option 1 - Anti-Malware Software
- Option 2 - Application Whitelisting
- Option 3 - Application Sandboxing

Please choose and complete only the option(s) below which you use in your organization.

Option 1 – Anti-Malware Software

Clause	Question	Comments/Evidence
6.1.1	Please provide the name of anti-virus solution which is installed on your devices.	
6.1.2	Has all anti-malware software been kept up to date (through daily automatic updates or through centrally managed deployment)?	
6.1.3	Is your anti-malware software configured to scan files automatically upon access (for example, when downloading and opening files, and accessing files on a network folder)?	
6.1.4	Are web pages scanned automatically upon access either by the web browser itself, the anti-malware software or by a third-party service?	

Option 2 – Application Whitelisting

Clause	Question	Comments/Evidence
6.2.1	Does the organisation maintain a current list of approved applications?	
6.2.2	Are only approved applications allowed to execute on devices?	
6.2.3	Are users able to install any applications that are not on the approved application list?	

Option 3 – Application Sandboxing

Clause	Question	Comments/Evidence
6.3	Are all application 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 a screenshot of your Anti-Virus solution showing status of definitions
Please provide a Screenshot of your AV on client PC showing the scheduled tasks including the daily scan

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.

Clause	Question	Comments/Evidence
7.1	Is all software installed on computers and network devices licensed and supported?	
7.2	Is all software removed from devices in scope when no longer supported?	
7.3	Is all software (Operating Systems and Applications) updated 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 a screenshot of Windows Update status

Approval

It is a requirement of the Scheme that a Senior Manager with authority within the organisation signs this application form and has approved that the information given is correct.

I am signing this on behalf of the organisation stated in this application form and state that the application form is completed in full and I have the correct level authorisation within the stated company to sign this. I agree to the terms and conditions of the assessment.

Name:

Position:

Date:

Signature:

Need Help?

If you need any help with your application, please contact our partners ID Cyber Solutions on their website:

https://apply.cyberessentials.online

Please complete and return application to

enquiries@centreforassessment.co.uk