

Cyber Essentials – Question List for Third Party IT Providers

We are applying for Cyber Essentials certification and need to confirm that the controls that are put in place by your company meet the requirements of the standard. Please answer all questions that are relevant to the services you provide to help us with our application.

Please answer all questions either as Yes or No or provide Notes as required. If you do not provide this service, please put N/A for your answer. If you answer 'yes' to say that you can provide a list, please can you provide this separately and return with this form. Thank you.

All supporting documentation for the scheme can be found at the link below if you need to refer to the requirements:

<https://www.ncsc.gov.uk/cyberessentials/resources>

CE Question	General Information		
	Question	Answer Type	Answer
Applicant Info	Is your organisation Cyber Essentials certified?	Yes / No	
Applicant Info	Have you read the Cyber Essentials Requirements for IT Infrastructure document? https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf	Yes / No	
Applicant Info	In the event that we are apply for Cyber Essentials Plus in the future will you give consent for us to scan any infrastructure that is owned by you?	Yes / No	
CE Question	Scope		
	Question	Answer Type	Answer
A2.4	Can you provide a list of all of laptops, computers and virtual desktops that you manage for us and include the details of their Operating Systems including editions and versions?	Yes / No (If Yes please provide list)	

A2.4.1	Can you provide a list of all thin clients that you manage for us and include the details of their Operating Systems including editions and versions?	Yes / No (If Yes please provide list)	
A2.5	Can you provide a list of servers that you manage for us including all virtual servers and their hosts (Hypervisors)? Please include their model and Operating Systems.	Yes / No (If Yes please provide list)	
A2.6	Can you provide a list of all tablets, mobile phones and other mobile devices that you manage for us? This list must include make and operating system for each device. Devices connecting to cloud services must be included.	Yes / No (If Yes please provide list)	
A2.7	Please could you provide a description of any networks that you provide to us, e.g. "Main Network at Head Office for administrative use", "Development Network at Malvern Office for testing software". You do not need to provide IP addresses or other technical information.	Notes	
A2.7	Can you confirm that these networks are segregated (using a boundary firewall or VLAN) from other clients that you provide services for?	Yes / No	
A2.8	Can you provide a list of make and model of any network equipment containing a firewall including all routers that you manage for us?	Yes / No (If Yes please provide list)	
A2.9	Can you provide a list of all cloud services that are subscribed to and managed on behalf of this company?	Yes / No (If Yes please provide list)	

CE Question	Office Firewalls and Internet Gateways (These apply to host-based firewalls on the OS and boundary firewalls)		
	Question	Answer Type	Answer
A4.1	Do you provide a firewall between the internal networks and the boundary?	Yes/No	
A4.1.1	Do we have a corporate VPN set up on our corporate devices that routes all traffic back to an internet boundary which you control?	Yes/No	
A4.1.1	Are our corporate device's software firewalls configured in the same manner as our boundary firewalls?	Yes/No	
A4.1.1	Have you configured any of our staff's BYOD to give them access to a corporate VPN that you manage?	Yes/No	
A4.2	Have the default passwords been changed on these firewalls?	Yes/No	
A4.2.1	Please can you describe the process for changing these passwords.	Notes	
A4.3	Please confirm that when selecting all firewall passwords including the admin password used for any IaaS solution have no maximum length and meet one of the following options. A – Minimum length of 8 characters and MFA Required B- Minimum length of 8 characters and a password deny list blocking common passwords C – Minimum length of 12 characters	Multi Choice A, B, C	

A4.4	What is the process you take if you believe a password has been compromised on a firewall or IaaS service that you manage?	Notes	
A4.5	Can you confirm that all services are disabled on firewalls and IaaS to prevent access from being advertised or accessible over the internet?	Yes/No	
A4.5.1	If services are enabled, can you confirm which ports are open and provide any details of why they need to be open to support our business case.	Notes	
A4.8	Can you make changes to the firewall settings remotely over the internet?	Yes/No	
A4.10	If you can make remote changes over the internet, is this protected by MFA or IP allow listing? Please provide details how this is protected.	Notes	
A4.11	Are software firewalls enabled on all desktop computers, laptops and servers if they are available?	Yes/No	
A4.12	Please provide a list of any operating systems in use that do not have software firewalls.	Notes	
CE	Secure Configuration		
Question	Question	Answer Type	Answer
A5.1	When setting up our laptops, desktop computers, thin clients, servers, tablets, mobile phones and cloud services did you disable or remove any software that came as standard from the vendor? If you did, how did you achieve this?	Notes	

A5.2	Can you provide us a list of accounts that access our devices?	Note	
A5.3	Have you changed all default passwords on all devices? Who is in control of these passwords (You? or have you handed details to us?).	Notes	
A5.4	Do we have any external services either hosted on an internal network or at a cloud data centre that is made available over the internet?	Yes / No	
A5.5	Where we have external services available over the internet, please confirm that it is protected by one of the following options: A – Minimum length of 8 characters and MFA B- Minimum length of 8 characters with a password deny list blocking common passwords when selecting C – Minimum length of 12 characters	Multi Choice A, B, C	
A5.6	If you access software or services over the internet, do you change passwords if you believe they have been compromised? Please explain the process.	Notes	
A5.7	If not using MFA to access external services, please describe how they are configured to protect against brute force attacks. If they are set to lock after a number of unsuccessful attempts, or the number of guesses are limited to a certain number during a certain time period, please provide that information.	Notes	

A5.8	When you provided our devices did you ensure “auto-run” or “auto-play” was disabled (to prevent software from running automatically on external media or when downloaded from the internet)?	Yes / No	
A5.9	When a device requires a user to be present, is there a locking mechanism in place to prevent access to the software and services installed on it?	Yes / No	
A5.10	Which methods are used to unlock the devices and what brute force protection is in place? Please include the PIN/password lengths and confirm whether these credentials can be used only to unlock the devices (and not to provide access to organisational data or services without further authorisation).	Notes	
CE	Security Update Management		
Question	Question	Answer Type	Answer
A6.1	Are all Operating Systems you provide properly licensed (including any subscriptions), supported by the vendor and still receiving regular vulnerability fixes?	Yes / No	
A6.1	Are all firewall or router devices that you supply to us still supported by the vendor and receiving regular firmware updates?	Yes / No	
A6.2 / A6.3	Are all installed applications that you provide properly licensed, still supported by the vendor and receiving regular vulnerability fixes?	Yes / No	

A6.2.1 - A6.2.4	Please can you list the Internet Browsers, Malware Protection Software, Email Applications and Office Applications installed on all devices that you have provided including current version numbers.	Notes	
A6.4 / A6.5	All high-risk or critical security updates should be applied within 14 days of release. This includes: Firmware on the following devices - Servers, Computers, Laptops, Tablets, Mobile Phones, Routers and Firewalls. Software updates including all Operating Systems and applications. Please confirm if you are using auto updates to achieve this task and where auto updates are not being used, how do you ensure this is achieved?	Notes	
A6.6	Do you remove applications that are no longer supported or no longer receive regular vulnerability fixes?	Yes / No	
A6.2 / A6.5	If you don't remove applications, can you provide a list of all installed applications that are on our devices?	Yes / No (If Yes please provide list)	

A6.7	Where we still have unsupported software on our machines, have these been moved onto their own sub-set? If this has happened, please describe how you have segregated this sub-set (for example by using a boundary firewall or VLAN)	Notes	
CE Question	Access Control		
	Question	Answer Type	Answer
A7.1	What is your process for account provision of all accounts that access our network? Who authorises these accounts?	Notes	
A7.2	Can you confirm that your employees do not use shared credentials to access our infrastructure? (shared meaning they are used by multiple persons)	Yes / No	
A7.3	How do you ensure you have deleted or disabled any accounts for staff that are no longer in your organisation?	Notes	
A7.4	How do you ensure that staff working on our network, only have the account privileges required to perform their tasks?	Notes	
A7.5	Do you have a formal process for granting administrative access to our network and can you confirm how this process is recorded?	Notes	
A7.6	Can you confirm that all administrators have separate standard user accounts? If they have standard user accounts associated with our network, what is the process to ensure separate accounts are used?	Notes	

A7.7	How do you ensure that your staff do not use their administrator accounts to carry out everyday tasks like email and web browsing; and only use their admin accounts to carry out admin specific tasks whilst operating on our network?	Notes	
A7.8 / A7.9	Do you formally track and review who has administrator accounts on our network?	Yes / No	
A7.10	Describe what controls are in place to protect accounts against brute force attacks. Please confirm if you use any of the listed methods below: - MFA - Throttling login attempts (include details of time / attempts) - Locking accounts after a number of failed attempts (include details of how many failed attempts)	Notes	
A7.11	Which Technical Controls are in place to manage the quality of our passwords. Please include details of any password complexity in place including minimum length, whether a password deny list for unacceptable passwords has been put in place and whether MFA is configured on all devices and services.	Notes	
A7.12	Please explain how you encourage your staff to pick passwords associated with our accounts that are unique and strong.	Notes	
A7.14	Is MFA enabled on all cloud services that you manage on our behalf?	Yes/No	

A7.15	Please list any cloud services which have not had MFA enabled because MFA has not been made available by the provider.	Notes	
A7.15	Please list any cloud services that do not have MFA enabled where MFA is available from the provider.	Notes	
A7.16	Has MFA been applied to all cloud service administrator accounts, used either by you or us?	Yes/No	
A7.17	Has MFA been applied to all cloud service standard user accounts, used either by you or us?	Yes/No	
CE	Malware Protection		
Question	Question	Answer Type	Answer
A8.1	Please list all devices that are protected by anti-malware software.	Notes	
A8.2 / A8.3	Is the anti-malware software set to update at least daily, scan files automatically on access and scan web pages you visit and warn of accessing malicious sites?	Yes / No	
A8.1	Please list all devices that are protected using application allow listing.	Notes	
A8.4 / A8.5	If using allow listing how is this enforced? For example, is there a technical solution like MDM where you set the approved list of applications that is provided by your company?	Notes	

Date_____
 Organisation Name_____
 Print Name_____
 Signature_____