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 that 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? | 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** |
| A2.6 | 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) |  |
| A2.6.1 | 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) |  |
| A2.7 | Can you provide a list of all tablets, mobile phones and other mobile devices that you manage for us? This list must include Operating System versions and model details for each device. | Yes / No  (If Yes please provide list) |  |
| A2.8 | Please could you provide a description of any networks that you provide to us eg Office LAN at head office at Birmingham head office. | Notes |  |
| A2.8 | Can you confirm that this / these networks are segregated through network segregation from other clients that you provide services for? | Yes / No |  |
| A2.9 | Can you provide a list of make and model of any network equipment that contain a firewall including all routers that you manage for us? | 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 |  |
| A4.2 | Have the default passwords been changed on these firewalls? | Yes/No |  |
| A4.3 | Are all firewall passwords you manage for us at least 8 characters in length and difficult to guess? | Yes/No |  |
| A4.4 | What is the process you take if you believe a password has been compromised on a firewall? | Notes |  |
| A4.5 | Can you confirm that all services are disabled on the firewall that prevent access from external devices on the internet? | Yes/No |  |
| A4.5.1 | If services are enabled, can you confirm which ports and services are open and provide any details of why they need to be open to support our business case. | Notes |  |
| A4.7 | Are firewalls configured to block all other services from being advertised to the internet? | Yes/No |  |
| 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, it this protected by 2FA or IP allow listing? Please provide details how this is protected. | Notes |  |
| A4.11 | Are all software firewalls enabled on desktop computers, laptops and servers if they are available? | Yes/No |  |
| A4.12 | Please provide a list of OS that does not have software firewalls. | Notes |  |
| **CE Question** | **Secure Configuration** | | |
| **Question** | **Answer Type** | **Answer** |
| A5.1 | When setting up our servers, computers, laptops and phones, 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 | If you provide domain access, can you provide us a list of user accounts that are currently active. | Yes / No  (If Yes please provide list) |  |
| A5.3 | Have you changed all default passwords on all devices to a non-guessable password of 8 characters or more? Who is control of these passwords (You or have you handed details to us). | Notes |  |
| A5.4 | Do all of your employees associated with our infrastructure have their own user and administrator accounts all with passwords of at least 8 characters and difficult to guess? | Yes / No |  |
| A5.5 | Do you access any software over the internet that has any of our data stored on? | Yes / No |  |
| A5.7 | If you access software over the internet, do you change passwords if you believe they have been compromised? Please explain the process | Notes |  |
| A5.8 | If you access software over the internet do your systems lock accounts after 10 or fewer unsuccessful accounts or throttle login attempts to no more than 10 within 5 minutes. | Yes / No |  |
| A5.9 | Do you have a password policy that tells your employees how to choose unguessable passwords, not to use the same password for multiple accounts and how they can record passwords? For example using a password manager. | Yes / No |  |
| A5.10 | When you provided our devices did you ensure “auto-run” or “auto-play” was disabled? | Yes / No |  |
| **CE Question** | **Security Update Management** | | |
| **Question** | **Answer Type** | **Answer** |
| A6.1 | Are all of the Operating Systems you provide licensed, supported by the vendor and still receiving regular security updates? | Yes / No |  |
| A6.2 | Are all of the installed applications that you provide, licensed, still supported and receiving regular security fixes? | Yes / No |  |
| A6.2.1 -A6.2.4 | Please can you list the Internet Browsers, Malware Protection Software, Email Applications and Office Applications that you have provided including current version numbers installed on all devices. | Notes |  |
| A6.4 / A6.5 | All high-risk or 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.  If you are responsible for this, how do you ensure this is achieved? | Notes |  |
| A6.5.1 / A6.5.2 | Auto Update should be used where possible. If this is not being used, please list the Operating Systems that that you are updating through other processes. | Notes |  |
| A6.6 | Do you removed any applications that are no longer supported or no longer receive regular fixes for security updates? | 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) |  |
| **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 access our infrastructure? | 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 control that staff working on our network, only have the account privileges required to perform their tasks? | Notes |  |
| A7.5 | What is the process for ensuring that all administrators are correctly trained and who authorises this level of access to our network? | Notes |  |
| A7.6 / 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 elevated privileges 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 | Do all of your accounts have 2FA enabled? | Yes / No |  |
| A7.11 | If no is this because 2FA is not available as standard? Please list the devices or systems it is not available for. | Yes/No  (Notes if No) |  |
| **CE Question** | **Malware Protection** | | |
| **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 now 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 |  |
| A8.1 | Please list all devices that are protected by sandboxing. | Notes |  |
| A8.6 | How do you ensure that sandboxed applications are unable to access data stores, peripherals and the local network? | Notes |  |

Date\_\_\_\_\_\_\_\_\_\_ Organisation Name\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Print Name\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_