Cyber Essentials Scheme

Report date: 2/1/2024
Applicant: Prestige Healthcare (London)Ltd,

Validated by: Robert Affutu-Nartey, Director

Thank you for applying for certification to the Cyber Essentials Scheme Self-Assessment.

Congratulations, you have been successful in your assessment under the Cyber Essentials scheme. Your certificate number is **2c65d99e-d1bb-466a-989a-6ea06aa2b999** and can be found here:

https://registry.blockmarktech.com/certificates/2c65d99e-d1bb-466a-989a-6ea06aa2b999/

Your insurance number is 0038191235 and it can be found here:

https://registry.blockmarktech.com/certificates/c5a31c87-24a3-43e3-b170-d2b7fb3bf553/
The insurance certificate has been set to private, but can be viewed when you register / log-in appropriately. We recommend keeping a hard copy or separate copy of your insurance certificate / schedule in case you need to make a claim and are unable to access your electronic copy. Both your Cyber Essentials and Insurance certificates have been emailed to you in separate messages as pdf attachments.

I include below the results from the form which you completed.

Applicant Answers

	Applicant Answers	Assessor Score
A1.1 Organisation Name What is your organisation's name? **The answer given in A1.1 is the name that will be displayed on your certificate and has a character limit of 150.** When an organisation wishes to certify subsidiary companies on the same certificate, the organisation can certify as a group and can include the subsidiaries' name on the certificate as long as the board member signing off the certificate has authority over all certified organisations. For example: The Stationery Group, incorporating The Paper Mill and The Pen House. It is also possible to list on a certificate where organisations are trading as other names. For example: The Paper Mill trading as The Pen House.	Prestige Healthcare (Group Holding) London Ltd	Compliant
A1.2 Organisation Type What type of organisation are you?	LTD - Limited Company (Ltd or PLC)	Compliant
A1.3 Organisation Number What is your organisation's registration number? Please enter the registered number only with **no spaces or other punctuation.** Letters (a-z) are allowed, but you need at least one digit (0-9). There is a 20 character limit for your answer. If you are applying for certification for more than one registered company, **please still enter only one organisation number.** If you have answered A1.2 with Government Agency, Sole Trader, Other Partnership, Other Club/Society or Other Organisation please enter "none". If you are registered in a country that does not issue a company number, please enter a unique identifier like a VAT or DUNS number.	13786488	Compliant
A1.4 Organisation Address	UK	Compliant

What is your organisation's address? Please provide the legal registered address for your organisation, if different from the main operating location.	Custom Fields: Country: United Kingdom Address Line 1: Prestige Healthcare (Group Holding) London Ltd Address Line 2: 5-7 Church Hill Road Town/City: East Barnet County: Hertfordshire Postcode: EN4 8SY	
A1.5 Organisation Occupation **What is your main business?** *Please summarise the main occupation of your organisation.*	Health	Compliant
A1.6 Website Address **What is your website address?** *Please provide your website address (if you have one). This can be a Facebook/LinkedIn page if you prefer.*	www.prestigehealthcare.co.uk	Compliant
A1.7 Renewal or First Time Application **Is this application a renewal of an existing certification or is it the first time you have applied for certification?** *If you have previously achieved Cyber Essentials, please select "Renewal". If you have not previously achieved Cyber Essentials, please select "First Time Application".*	New Application	Compliant
A1.8 Reason for Certification **What are the two main reasons for applying for certification?** *Please let us know the two main reasons why you are applying for certification. If there are multiple reasons, please select the two that are most important to you. This helps us to understand how people are using our certifications.*	To Give Confidence to Our Customers Custom Fields: Applicant Notes: To Generally Improve Our Security Secondary Reason: Required for Commercial Contract	Compliant
A1.8.1 Contracting Organisation **Who is the commercial contracting organisation?**	NHS Share Business Services	Compliant

Please provide the name of the contracting organisation.		
A1.9 CE Requirements Document **Have you read the 'Cyber Essentials Requirements for IT Infrastructure' document?** *Document is available on the NCSC Cyber Essentials website and should be read before completing this question set. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*	Yes	Compliant
A1.10 Cyber Breach **Can IASME and their expert partners contact you if you experience a cyber breach?** *We would like feedback on how well the controls are protecting organisations. If you agree to this then please email security@iasme.co.uk if you do experience a cyber breach. IASME and expert partners will then contact you to find out a little more but all information will be kept confidential.*	Yes	Compliant
A2.1 Assessment Scope **Does the scope of this assessment cover your whole organisation?** **Please note: Your organisation is only eligible for free cyber insurance if your assessment covers your whole company, if you answer "No" to this question you will not be invited to apply for insurance.** *Your whole organisation includes all divisions, people and devices which access your organisation's data and services.*	Yes	Compliant
A2.3 Geographical Location **Please describe the geographical locations of your business which are in the scope of this assessment.** *You should provide either a broad description (i.e. All UK offices) or simply list the locations in scope (i.e. Manchester and Glasgow retail stores).*	PHC has two offices in the UK the main HO in East Barnet and a small satellite office at Gatwick	Compliant
A2.4 End User Devices Please list the quantities and operating	Teamviewer Name Machine name Model	Compliant Assessor Notes:

systems for your laptops, desktops and virtual desktops within the scope of this assessment. **Please Note: You must include make and operating system versions for all devices.** **All user devices declared within the scope of the certification only require the make and operating system to be listed.We have removed the requirement for the applicant to list the model of the device.Devices that are connecting to cloud services must be included.A scope that does not include end user devices is not acceptable.** *You need to provide a summary of all laptops, computers, virtual desktops and their operating systems that are used for accessing organisational data or services and have access to the internet.For example, "We have 25 DELL laptops running Windows 10 Professional version 20H2 and 10 MacBook laptops running MacOS Ventura".Please note, the edition and feature version of your Windows operating systems are required.This applies to both your corporate and user owned devices (BYOD). You do not need to provide serial numbers, mac addresses or further technical information.*	OS Build AVG / Malwarebytes EDR DESKTOP-70C1KCE RM1 DESKTOP-70C1KCE HP 290 G9 Windows 11 Pro 22H2 (OS Build 22621.2715) Protected DESKTOP-91UCT7T RM2 DESKTOP-91UCT7T HP 290 G9 Windows 11 Pro 22H2 (OS Build 22621.2715) Protected PHC DORA DESKTOP-1U72QA1 Lenovo neo 50 Windows 10 Pro 22H2 (OS Build 19045.3693) Protected PHC MICHELE DESKTOP-419K084 Lenovo neo 50 Windows 10 Pro 22H2 (OS Build 19045.3693) Protected PHC PENNY DESKTOP-515KT8P Lenovo neo 50 Windows 10 Pro 22H2 (OS Build 19045.3693) Protected PHC ROBERT DESKTOP-62JNB7S Lenovo neo 50 Windows 11 Pro 22H2 (OS Build 22621.2715) Protected PHC SHOP DESKTOP-670EEEB Lenovo neo 50 Windows 11 Pro 22H2 (OS Build 22621.2715) Protected PHC SUE DESKTOP-C4D82M9 Lenovo neo 50 Windows 11 Pro 22H2 (OS Build 22621.2715) Protected PHC SERVER PHC-SRV DELL T440 Windows Server 2019 1809 (OS Build 17763.5122) Protected	In support at the time of the assessment.
A2.4.1 Thin Client Devices **Please list the quantity of thin clients within scope of this assessment. Please include make and operating systems.** *Please provide a summary of all the thin clients in scope that are connecting to organisational data or services*	PHC has no thin client devices.	Compliant

(Definitions of which are in the 'CE Requirements for Infrastructure document' linked in question A1.9). *Thin clients are commonly used to connect to a Virtual Desktop Solution.* ***Thin clients are a type of very simple computer holding only a base operating system which are often used to connect to virtual desktops. Thin clients can connect to the internet, and it is possible to modify some thin clients to operate more like PCs, and this can create security complications. Cyber Essentials requires thin clients be supported and receiving security updates.*** *https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*		
A2.5 Server Devices **Please list the quantity of servers, virtual servers and virtual server hosts (hypervisor). You must include the operating system.** *Please list the quantity of all servers within scope of this assessment.* *For example, 2 x VMware ESXI 6.7 hosting 8 virtual windows 2016 servers; 1 x MS Server 2019; 1 x Redhat Enterprise Linux 8.3*	1 x Dell T440 Fileserver Windows Server 2019 Version	Compliant Assessor Notes: In support at the time of the assessment.
A2.6 Mobile Devices Please list the quantities of tablets and mobile devices within the scope of this assessment. **Please Note** You must include make and operating system versions for all devices. All user devices declared within the scope of the certification only require the make and operating system to be listed. We have removed the requirement for the applicant to list the model of the device. **Devices that are connecting to cloud services must be included in the scope that does not include end user devices is not acceptable.** *All tablets and mobile devices that are used for accessing organisational data or services and have access to the internet must be included in the scope of the assessment. This applies to both corporate and user owned devices (BYOD).You are not required to list any serial numbers, mac addresses or other technical information.*	Personal phones just with work emails. Name IMEI Number Software Update Kevin Van Dort IMEI 356728118957543 IOS 17.1.2 Joshua Ogantard IMEI 351393987409368 Android 14 (One UI 6.0)Samsung Version 6, Security patch level: November 23 Paul Outred IMEI 351401235544314 Motorola TITPS33.75-96-1-2 November 23 Malcolm Fox IMEI 354873091179368 IOS 17.1.2 Linda Rogers ImEI 356781405150595 IOS 17.1.2 Colin Hurley IMEI 354356423596756 IOS 17.1.2 Lucille Cowell IMEI 355546532232124 IOS 17.1.2 Goodness Ajaero IMEI 350146811995254	Compliant Assessor Notes: In support at the time of the assessment.

	Android 14 (One UI 6.0)Samsung Version 6, Security patch level: November 23 Robert Affutu-Nartey IMEI 358795288200580 IOS 17.1.2	
A2.7 Networks **Please provide a list of your networks that will be in the scope for this assessment.** *You should include details of each network used in your organisation including its name, location and its purpose (i.e. Main Network at Head Office for administrative use, Development Network at Malvern Office for testing software, home workers network - based in UK).* *You do not need to provide IP addresses or other technical information.* *For further guidance see the Home Working section in the 'CE Requirements for Infrastructure Document'.* https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf	Main Network at East Barnet (Head Office for administrative use)	Compliant
A2.7.1 Home Workers **How many staff are home workers?** *Any employee that has been given permission to work at home for any period of time at the time of the assessment, needs to be classed as working from home for Cyber Essentials.* *For further guidance see the Home Working section in the 'CE Requirements for Infrastructure Document'.* *https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*	Robert & 3 part time medical consultancy doing work in 2 NHS hospitals covering for each other in the orthotics department using 2 NHS laptops onsite in the hospital and from time to time may connect to PHC fileserver using Draytek SSL VPN.	Compliant
A2.8 Network Equipment **Please provide a list of your network equipment that will be in scope for this assessment (including firewalls and routers). You must include make and model of each device listed.** *You should include all equipment that controls the flow of data, this will be your routers and firewalls.*	PHC have a secure broadband feed from BT to our business Draytek 2865 firmware 4.4.3.1 BT (VPN and Content filtering)	Compliant

You do not need to include switches or wireless access points that do not contain a firewall or do not route internet traffic. *If you don't have an office and do not use network equipment, instead you are relying on software firewalls please describe in the notes field.* *You are not required to list any IP addresses, MAC addresses or serial numbers.*		
A2.9 Cloud Services Please list all of your cloud services that are in use by your organisation and provided by a third party. **Please note cloud services cannot be excluded from the scope of CE.** *You need to include details of all of your cloud services. This includes all types of services - IaaS, PaaS and SaaS. Definitions of the different types of Cloud Services are provided in the 'CE Requirements for Infrastructure Document'.* https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf	Microsoft Office 365	Compliant
A2.10 Responsible Person **Please provide the name and role of the person who is responsible for managing your IT systems in the scope of this assessment.** *This person must be a member of your organisation and cannot be a person employed by your outsourced IT provider.*	Robert Affutu-Nartey Custom Fields: Responsible Person Role: Director	Compliant
A3.1 Head Office **Is your head office domiciled in the UK or Crown Dependencies and is your gross annual turnover less than £20m?** *This question relates to the eligibility of your organisation for the included cyber insurance*.	Yes	Compliant
A3.2 Cyber Insurance **If you have answered "yes" to the last question then your organisation is eligible for the included cyber insurance if you**	Opt-In	Compliant

gain certification. If you do not want this insurance element please opt out here. *There is no additional cost for the insurance. You can see more about it at https://iasme.co.uk/cyber-essentials/cyber-liability-insurance/*		
A3.3 Total Gross Revenue **What is your total gross revenue? Please provide figure to the nearest £100K. You only need to answer this question if you are taking the insurance.** *The answer to this question will be passed to the insurance broker in association with the cyber insurance you will receive at certification. Please be as accurate as possible - figure should be to the nearest £100K.*	1.1 million	Compliant
A3.4 Insurance Email Contact **What is the organisation email contact for the insurance documents? You only need to answer this question if you are taking the insurance.** *The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification and they will use this to contact you with your insurance documents and renewal information.*	robert@prestigehealthcare.co.uk	Compliant
A4.1 Boundary Firewall **Do you have firewalls at the boundaries between your organisation's internal networks, laptops, desktops, servers and the internet?** *You must have firewalls in place between your office network and the internet.*	Yes Custom Fields: Applicant Notes: Draytek 2865 Firmware 4.4.3.1 BT latest release (VPN and Content filtering)	Compliant
A4.1.1 Off Network Firewalls **When your devices (including computers used by homeworkers) are being used away from your workplace (for example, when they are not connected to your internal network), how do you ensure they are protected?** You should have firewalls in place for home-based workers. If those users are not using a Corporate Virtual Private Network (VPN) connected to your office network, they will need to rely on the software firewall included in the operating	All remote worker connect to head office use DrayTek Smart VPN Client with SSL connection and have up to date Anti-Virus installed on their home pc or laptop.	Compliant

system of their device.		
A4.2 Firewall Default Password **When you first receive an internet router or hardware firewall device, it may have had a default password on it. Have you changed all the default passwords on your boundary firewall devices?** *The default password must be changed on all routers and firewalls, including those that come with a unique password pre-configured (i.e. BT Business Hub, Draytek Vigor 2865ac).* *When relying on software firewalls included as part of the operating system of your end user devices, the password to access the device will need to be changed.*	Yes Custom Fields: Applicant Notes: Applicant Notes: password is 14 characters with upper / lower case and numbers	Compliant
A4.2.1 Firewall Password Change Process **Please describe the process for changing your firewall password?** **Home routers not supplied by your organisation are not included in this requirement.** *You need to understand how the password on your firewall(s) is changed. Please provide a brief description of how this is achieved.*	Robert the directors would send an email to our IT support company asking for the Draytek router password to be change for any reason and the IT company would logon using TeamViewer and make the password change and send back confirmation the password has been changed on the router the IT company would keep a record of this change and any reason for the change also the directors would keep a record as to why the change was required.	Compliant
A4.3 Firewall Password Configuration Is your new firewall password configured to meet the 'Password-based authentication' requirements? Please select the option being used. A. Multi-factor authentication, with a minimum password length of 8 characters and no maximum length B. Automatic blocking of common passwords, with a minimum password length of 8 characters and no maximum length C. A minimum password length of 12 characters and no maximum length D. None of the above, please describe *Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the new section about password-based authentication in the 'Cyber Essentials*	0: C. A password minimum length of 12 characters and no maximum length Custom Fields: Applicant Notes: password is 14 characters with upper / lower case and numbers	Compliant

Requirements for IT Infrastructure' document. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf		
A4.4 Firewall Password Issue **Do you change your firewall password when you know or suspect it has been compromised?** *Passwords may be compromised if there has been a virus on your system or if the manufacturer notifies you of a security weakness in their product. You should be aware of this and know how to change the password if this occurs.* *When relying on software firewalls included as part of the operating system of your end user devices, the password to access the device will need to be changed.*	Yes Custom Fields: Applicant Notes: Yes if any of the staff feel a possible infringement in security they will speak to Robert who will inform IT company to change the relevant passwords. PHC have cloud security monitoring virus / malware and the IT company will be email of any malware / virus found on the system. We can reset our own Office 365 password if required by following the Microsoft procedure.	Compliant
A4.5 Firewall Services **Do you have any services enabled that can be accessed externally through your internet router, hardware firewall or software firewall?** *At times your firewall may be configured to allow a system on the inside to become accessible from the internet (for example: a VPN server, a mail server, an FTP server or a service that is accessed by your customers). This is sometimes referred to as "opening a port". You need to show a business case for doing this because it can present security risks. If you have not enabled any services, answer "No". By default, most firewalls block all services.*	Yes Custom Fields: Applicant Notes: DrayTek router only use manaufacturs SSL VPN Client.	Compliant
A4.5.1 Firewall Documented Business Case **Do you have a documented business case for all of these services?** *The business case should be documented and recorded. A business case must be signed off at board level and associated risks reviewed regularly.*	Yes Custom Fields: Applicant Notes: The business case for allowing a smart SSL VPN to access PHC fileserver to gain access to a SQL Microsoft access database for ordering orthotics equipment / aids for patients in PHC clinics at the hospitals its been agreed and approved by the owner Robert as a need for running his clinics.	Compliant
A4.6 Firewall Service Process **If you do have services enabled on your firewall, do you have a process to ensure**	Robert will review his electronic file focus on any changes to the company firewall and reasons / case for any changes to be made and will discuss with our current IT	Compliant

they are disabled in a timely manner when they are no longer required? A description of the process is required. *If you no longer need a service to be enabled on your firewall, you must remove it to reduce the risk of compromise. You should have a process that you follow to do this (i.e. when are services reviewed, who decides to remove the services, who checks that it has been done?).*	support company regarding risks and any security issues before any instruction is given to make these changes. Robert reviews all IT issues monthly and documents changing to the company setup a long side his IT support company. If a change is required, then IT support company will carry out the change and email confirmation will be sent to Robert of the change has taken place.	
A4.7 Firewall Service Block **Have you configured your boundary firewalls so that they block all other services from being advertised to the internet?** *By default, most firewalls block all services from inside the network from being accessed from the internet, but you need to check your firewall settings.*	Yes Custom Fields: Applicant Notes: NO ports are open on the DrayTek router you cannot even get a ping on the external ip address and the router can only be manager from within the internal network the only services PHC are using is SSL VPN for remote workers.	Compliant
A4.8 Firewall Remote Configuration **Are your boundary firewalls configured to allow access to their configuration settings over the internet?** *Sometimes organisations configure their firewall to allow other people (such as an IT support company) to change the settings via the internet.* *If you have not set up your firewalls to be accessible to people outside your organisations or your device configuration settings are only accessible via a VPN connection, then answer "no" to this question.*	No Custom Fields: Applicant Notes: Can only be access from the internal network. Our IT support company will logon to fileserver using TeamViewer and make changes on fileserver.	Compliant
A4.11 Software Firewalls **Do you have software firewalls enabled on all of your computers, laptops and servers?** *Your software firewall must be configured and enabled at all times, even when sitting behind a physical/virtual boundary firewall in an office location. You can check this setting on Macs in the Security & Privacy section of System Preferences. On Windows laptops you can check this by going to Settings and searching for "Windows firewall". On Linux try "ufw status".*	Yes Custom Fields: Applicant Notes: software firewall is configured and enabled at all times, even when sitting behind a physical/virtual boundary firewall.	Compliant

A5.1 Removed Unused Software **Where you are able to do so, have you removed or disabled all the software and services that you do not use on your laptops, desktop computers, thin clients, servers, tablets, mobile phones and cloud services? Describe how you achieved this.** *You must remove or disable all applications, system utilities and network services that are not needed in day-to-day use. You need to check your cloud services and disable any services that are not required for day-to-day use.* *To view your installed applications:* *1. Windows by right clicking on Start ? Apps and Features* *2. macOS open Finder -> Applications* *3. Linux open your software package manager (apt, rpm, yum).*	1)Any new pcs / laptops are all windows based and any non-company applications will be removed before joining the company network. 2)Robert the director has asked our IT support company to check each computer at least every 2 months for any outdated software and report back to Robert which he will issue an instruction for the software to be removed from the pc and confirm by email back to him. 3)PHC staff only use a very limited software applications being approved by the director which is mainly standard industry software which are all subscription base. Office 365 & Sage 50 accounts also subscription base.	Compliant
A5.2 Remove Unrequired User Accounts **Have you ensured that all your laptops, computers, servers, tablets, mobile devices and cloud services only contain necessary user accounts that are regularly used in the course of your business?** *You must remove or disable any user accounts that are not needed in day-to-day use on all devices and cloud services.* *You can view your user accounts* *1. Windows by righting-click on Start -> Computer Management -> Users,* *2. macOS in System Preferences -> Users & Groups* *3. Linux using ""cat /etc/passwd""*	Yes Custom Fields: Applicant Notes: When an employee leaves the organization the director/owner will let the relevant IT person know approx. a week before leaving in an email asking for the user account to be backed up / closed all accounts (internal network accounts / cloud accounts). The IT person will confirm this has been actioned and email back to the directors.	Compliant
A5.3 Change Default Password **Have you changed the default password for all user and administrator accounts on all your desktop computers, laptops, thin clients, servers, tablets and mobile phones that follow the Password-based authentication requirements of Cyber Essentials?** *A password that is difficult to guess will be unique and not be made up of common or predictable words such as "password" or "admin" or include predictable number sequences such as "12345".*	Yes Custom Fields: Applicant Notes: Our fileserver server policy part of our PHC domain requires at least 14 characters uppercase and lowercase and letters and numbers. Any external cloud admin accounts like our Office 365 require MFA on the users using the software	Compliant

A5.4 Internally Hosted External Services **Do you run external services that provides access to data (that shouldn't be made public) to users across the internet?** *Your business might run software that allows staff or customers to access information across the internet to an external service hosted on the internal network, cloud data centre or IaaS cloud service. This could be a VPN server, a mail server, or an internally hosted internet application(SaaS or PaaS) that you provide to your customers as a product. In all cases, these applications provide information that is confidential to your business and your customers and that you would not want to be publicly accessible.*	No Custom Fields: Applicant Notes: PHC do not host any external services that hold or provides access to company data	Compliant
A5.8 Auto-Run Disabled **Is "auto-run" or "auto-play" disabled on all of your systems?** This is a setting on your device which automatically runs software on external media or downloaded from the internet. *It is acceptable to choose the option where a user is prompted to make a choice about what action will occur each time they insert a memory stick. If you have chosen this option, you can answer yes to this question.*	Yes Custom Fields: Applicant Notes: Yes auto-run or auto-play is disabled on all pcs / any memory stick loaded with any application will need the help from our external IT company because of the PHC domain policy restricting running applications and anti-malware / anti-virus will auto scan any CD/DVD/Memory stick inserted into the pc.	Compliant
A5.9 Device Locking **When a device requires a user to be present, do you set a locking mechanism on your devices to access the software and services installed?** *Device locking mechanisms such as biometric, password or PIN, need to be enabled to prevent unauthorised access to devices accessing organisational data or services.*	Yes Custom Fields: Applicant Notes: All windows computers are set to lock after 10 minutes of no usage and all computers need user login id / password to unlock.	Compliant
A5.10 Device Locking Method **Which method do you use to unlock the devices?** Please refer to Device Unlocking Credentials paragraph found under Secure Configuration in the Cyber Essentials Requirements for IT Infrastructure document for further	PHC use password method and all staff have a minimum password at least 12 characters.	Compliant

information. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf The use of a PIN with a length of at least six characters can only be used where the credentials are just to unlock a device and does not provide access to organisational data and services without further authentication.		
A6.1 Supported Operating System **Are all operating systems on your devices supported by a vendor that produces regular security updates?** **If you have included firewall or router devices in your scope, the firmware of these devices is considered to be an operating system and needs to meet this requirement.** *Older operating systems that are out of regular support include Windows 7/XP/Vista/ Server 2003, mac OS Mojave, iOS 12, iOS 13, Android 8 and Ubuntu Linux 17.10.* *It is important you keep track of your operating systems and understand when they have gone end of life (EOL). Most major vendors will have published EOL dates for their operating systems and firmware.*	Yes Custom Fields: Applicant Notes: All pcs / fileserver is set to regular windows updates from Microsoft. PHC only have Microsoft windows server 2019 & Microsoft windows 10 & 11 professional.	Compliant
A6.2 Supported Software **Is all the software on your devices supported by a supplier that produces regular fixes for any security problems?** *All software used by your organisation must be supported by a supplier who provides regular security updates. Unsupported software must be removed from your devices. This includes frameworks and plugins such as Java, Adobe Reader and .NET.*	Yes Custom Fields: Applicant Notes: All software applications get regular updates from Microsoft Office 365 / Adobe Reader / Sage. 100% of PHC software is subscription based so is supported by the manufacturer and regular updates.	Compliant
A6.2.1 Internet Browsers **Please list your internet browser(s). The version is required.** *Please list all internet browsers installed on your devices, so that the Assessor can understand your setup and verify that they are in support.* *For example: Chrome Version 102, Safari Version 15.*	Google Chrome Version 119.0.6045.200 (Official Build) (64-bit) Microsoft Edge Version 119.0.2151.93 (Official build) (64-bit)	Compliant Assessor Notes: In support at the time of the assessment.

A6.2.2 Malware Protection **Please list your Malware Protection software.** **The version is required.** *Please list all malware protection and versions you use so that the Assessor can understand your setup and verify that they are in support.* *For example: Sophos Endpoint Protection V10, Windows Defender, Bitdefender Internet Security 2020.*	Malwarebytes (endpoint detection response (EDR) version 1.2.0.389 AVG Internet security software version 23.10.3306 (build 23.10.8563.808) virus derfinition version 231205-34	Compliant
A6.2.3 Email Application **Please list your email applications installed on end user devices and server. The version is required.** *Please list all email applications and versions you use so that the Assessor can understand your setup and verify that they are in support.* *For example: MS Exchange 2016, Outlook 2019.*	Office 365 Exchange on Microsoft datacentre All users have office premium account with Outlook 365 client on work pcs.	Compliant
A6.2.4 Office Applications **Please list all office applications that are used to create organisational data.** **The version is required.** *Please list all office applications and versions you use so that the Assessor can understand your setup and verify that they are in support.* *For example: MS 365; Libre office, Google workspace, Office 2016.*	All users have Microsoft office 365 with Outlook, Word, Access, Excel, Power Point, Publisher.	Compliant
A6.3 Software Licensing **Is all software licensed in accordance with the publisher's recommendations?** *All software must be licensed. It is acceptable to use free and open source software as long as you comply with any licensing requirements.* *Please be aware that for some operating systems, firmware and applications, if annual licensing is not purchased, they will not be receiving regular security updates.*	Yes Custom Fields: Applicant Notes: All PHC software is licensed with Microsoft or on subscription with Microsoft Office 365 / Sage subscription / AVG Internet Security subscription.	Compliant
A6.4 Security Updates - Operating	Yes	Compliant

System **Are all high-risk or critical security updates for operating systems and router and firewall firmware installed within 14 days of release?** *You must install all high and critical security updates within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question. You are not required to install feature updates or optional updates in order to meet this requirement.* *This requirement includes the firmware on your firewalls and routers.*		
A6.4.1 Auto Updates - Operating System **Are all updates applied for operating systems by enabling auto updates?** *Most devices have the option to enable auto updates. This must be enabled on any device where possible.*	Yes	Compliant
A6.4.2 Manual Updates - Operating System **Where auto updates are not being used, how do you ensure all high-risk or critical security updates of all operating systems and firmware on firewalls and routers are applied within 14 days of release?** *It is not always possible to apply auto updates, this is often the case when you have critical systems or servers and you need to be in control of the updating process.* *Please describe how any updates are applied when auto updates are not configured.* *If you only use auto updates, please confirm this in the notes field for this question.*	All PHC software are auto updates as new builds are released by the software companies. Our IT company keep an eye on updates in case they stop working and does regular checks on build versions of the software with their TeamViewer monitoring proactively monitor important aspects of your devices and ensure a healthy and secure IT infrastructure.	Compliant
A6.5 Security Updates - Applications **Are all high-risk or critical security updates for applications (including any associated files and any plugins such as Java, Adobe Reader and .Net.) installed within 14 days of release?** *You must install any such updates within 14 days in all circumstances.* *If you cannot achieve this requirement at all times, you will not achieve compliance to this question.*	Yes	Compliant

You are not required to install feature updates or optional updates in order to meet this requirement, just high-risk or critical security updates.		
A6.5.1 Auto-Updates - Applications **Are all updates applied on your applications by enabling auto updates?** *Most devices have the option to enable auto updates. Auto updates should be enabled where possible.*	Yes	Compliant
A6.5.2 Manual Updates - Applications **Where auto updates are not being used, how do you ensure all high-risk or critical security updates of all applications are applied within 14 days of release?** *It is not always possible to apply auto updates, this is often the case when you have critical systems or applications and you need to be in control of the updating process.* *Please describe how any updates are applied when auto updates are not configured.* *If you only use auto updates, please confirm this in the notes field for this question.*	PHC does not have any software that requires manual updates at present. If any staff have issues with the applications, they will log a support call to our IT support company. PHC have a very limited software list only three applications which are all have built in auto updates like Office365 / Sage / Windows 10 or 11 Professional.	Compliant
A6.6 Unsupported Software Removal **Have you removed any software installed on your devices that is no longer supported and no longer receives regular updates for security problems?** *You must remove older software from your devices when it is no longer supported by the manufacturer. Such software might include older versions of web browsers, operating systems, frameworks such as Java and Flash, and all application software.*	Yes Custom Fields: Applicant Notes: PHC use a limited number of approved industry standard software which is supported by the manufacturer.	Compliant
A6.7 Unsupported Software Segregation **Where you have a business need to use unsupported software, have you moved the devices and software out of scope of this assessment? Please explain how you achieve this.** *Software that is not removed from devices when it becomes un-supported will need to be placed onto its own sub-set with no internet access.*	No unsupported software.	Compliant

If the out-of-scope subset remains connected to the internet, you will not be able to achieve whole company certification and an excluding statement will be required in question A2.2. *A sub-set is defined as a part of the organisation whose network is segregated from the rest of the organisation by a firewall or VLAN.*		
A7.1 User Account Creation **Are your users only provided with user accounts after a process has been followed to approve their creation? Describe the process.** *You must ensure that user accounts (such as logins to laptops and accounts on servers) are only provided after they have been approved by a person with a leadership role in the business.*	Yes, all approvals are by Robert the director and the owner of the business. Who send an email to the IT company of when the new member of staff is joining and what applications / access to PHC network is needed i.e. job role: Accounts Dept / Admin Dept.	Compliant
A7.2 Unique Accounts **Are all your user and administrative accounts accessed by entering a unique username and password?** *You must ensure that no devices can be accessed without entering a username and password.* **Accounts must not be shared.**	Yes	Compliant
A7.3 Leavers Accounts **How do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation?** *When an individual leaves your organisation you need to stop them accessing any of your systems.*	When an employee leaves the organization the director/owner will let the relevant IT person know approx. a week before leaving in an email asking for the account to be backed up / closed. The IT person will confirm this has been actioned and email back to the director.	Compliant
A7.4 User Privileges **Do you ensure that staff only have the privileges that they need to do their current job? How do you do this?** *When a staff member changes job role, you may also need to change their permissions to only access the files, folders and applications that they need to do their day to day work.*	The company is broken up into Admin, Accounts, Personnel, Sales, General and the PHC has various security groups that the staff can be a member of that group to have access to that information.	Compliant
A7.5 Administrator Approval	The owner makes the decision regarding Administrator rights no one has	Compliant

Do you have a formal process for giving someone access to systems at an "administrator" level and can you describe this process? *You must have a process that you follow when deciding to give someone access to systems at administrator level. This process might include approval by a person who is an owner/director/trustee/partner of the organisation.*	Administrator rights within the company only our IT company which we have worked with for the last 5 years and its Robert decision.	
A7.6 Use of Administrator Accounts **How does your organisation make sure that separate accounts are used to carry out administrative tasks (such as installing software or making configuration changes)?** *You must use a separate administrator account from the standard user account, when carrying out administrative tasks such as installing software. Using administrator accounts all-day-long exposes the device to compromise by malware. Cloud service administration must be carried out through separate accounts.*	No one in the PHC domain / on the PHC internal network has administrative rights including the director. Our outsourced IT company deals with any new software to be loaded onto the network / any changes to access rights into any folders / files on the instruction from the one owner / Director of the company by written email requesting the change to the system. Our outsourced IT company has a separate administrator account.	Compliant
A7.7 Managing Administrator Account Usage **How does your organisation prevent administrator accounts from being used to carry out every day tasks like browsing the web or accessing email?** *This question relates to the activities carried out when an administrator account is in use.* *You must ensure that administrator accounts are not used to access websites or download email. Using such accounts in this way exposes the device to compromise by malware. Software and update downloads should be performed as a standard user and then installed as an administrator. You might not need a technical solution to achieve this, it could be based on good policy, procedure and regular training for staff.*	All users are standard domain users that only have access to directories & files on PHC fileserver and controlled by the member of groups / policy which give the access to different parts of the system but will limit any user from installing any applications / our endpoint protections stops users from downloading malware / virus / blocks websites and is cloud monitored and will isolate the workstation from the network if any breach on security.	Compliant
A7.8 Administrator Account Tracking **Do you formally track which users have administrator accounts in your organisation?** *You must track all people that have been granted administrator accounts.*	Yes Custom Fields: Applicant Notes: Robert the director has a permission change form and electronic file with the user login name, date of permission change, a note section as to why the	Compliant

	reason for giving Administrator rights, the duration i.e. permanent or a temporary arrangement, the date for the changes to take place, instruction date & time for email form to IT company from PHC to make the changes and a confirmation back to Robert that the changes have taken place. Robert has a permission change form 1) Rights Given = 2) Duration = permanent or a temporary 3) Section as to why 4) Changes to take place by 5) Email to IT company date 6) Email back from IT to confirm	
A7.9 Administrator Access Review **Do you review who should have administrative access on a regular basis?** *You must review the list of people with administrator access regularly. Depending on your business, this might be monthly, quarterly or annually. Any users who no longer need administrative access to carry out their role should have it removed.*	Yes Custom Fields: Applicant Notes: Robert the director will review his electronic file on Administrator rights on a monthly basis focusing on Administrator access rights given and any changes Robert will send a permission change form to IT company to complete the changes.	Compliant
A7.10 Brute Force Attack Protection **Describe how you protect accounts from brute-force password guessing in your organisation?** *A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.* *Information on how to protect against brute-force password guessing can be found in the Password-based authentication section, under the User Access Control section in the 'Cyber Essentials Requirements for IT Infrastructure* *https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*	We have now implemented Brute force attack prevention on Malwarebytes EDR Block IP addresses that exceed a threshold of 5 x invalid login attempts. https://www.malwarebytes.com/business/solutions/brute-force-protection We have account lockout policy on our windows server 2019 after 5 failed attempts the account will be lock until a reset by our IT Company.	Compliant
A7.11 Password Quality **Which technical controls are used to manage the quality of your passwords within your organisation?** *Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the new section about password-based*	PHC server policy part of our domain requires at least 12 characters or greater Michael requires staff to change their password every 3 months and to choose a new password with 1-Uppercase letter / 2-Lowercase letters / 3-Numbers / 4-Special character or characters.	Compliant

authentication in the 'Cyber Essentials Requirements for IT Infrastructure' document. *https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*		
A7.12 Password Creation Advice **Please explain how you encourage people to use unique and strong passwords.** *You need to support those that have access to your organisational data and services by informing them of how they should pick a strong and unique password.* *Further information can be found in the password-based authentication section, under the User Access Control section in the Cyber Essentials Requirements for IT Infrastructure* *document.* *https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*	Robert has instigated that all the staff pick two or three unrelated words and change some of the letters into numbers and also use Special character or characters in the password must be 12 characters or greater.	Compliant
A7.13 Password Policy **Do you have a process for when you believe the passwords or accounts have been compromised?** *You must have an established process that details how to change passwords promptly if you believe or suspect a password or account has been compromised.*	Yes Custom Fields: Applicant Notes: Robert keeps a file on any issues with changing passwords on external agencies like HMRC / Microsoft Office365 (i.e. staff leaving that had access to these agencies) & our external IT company keep records of any possible password compromised and this will originate from if any of the staff feel a possible infringement in security they will speak to Robert who will inform IT company to change the relevant passwords.	Compliant
A7.14 MFA Enabled **Do all of your cloud services have multi-factor authentication (MFA) available as part of the service?** *Where your systems and cloud services support multi-factor authentication (MFA), for example, a text message, a one time access code, notification from an authentication app, then you must enable for all users and administrators. For more information see the NCSC's guidance on MFA.* *Where a cloud service does not have its own MFA solution but can be configured to link to another cloud service to provide MFA, the link will need to be configured. A lot of cloud services use another cloud*	Yes Custom Fields: Applicant Notes: On some not all. Office 365 / TeamViewer for support / Cloud Anti-Virus / Anti- Malware protection / HMRC / two-factor authentication.	Compliant

service to provide MFA. Examples of cloud services that can be linked to are Azure, MS365, Google Workspace.		
A7.16 Administrator MFA **Has MFA been applied to all administrators of your cloud services?** *It is required that all administrator accounts on cloud service must apply multi-factor authentication in conjunction with a password of at least 8 characters.*	Yes Custom Fields: Applicant Notes: IT Support Company = Office 365 MFA / TeamViewer MFA / Malwarebytes Nebula Console MFA . AKDP staff = HMRC / Companies House. Our IT company have confirmed in writing that all the password used are 18 characters or greater and 1-Uppercase letter / 2-Lowercase letters / 3-Numbers / 4-Special character or characters.	Compliant
A7.17 User MFA **Has MFA been applied to all users of your cloud services?** *All users of your cloud services must use MFA in conjunction with a password of at least 8 characters.*	Yes	Compliant
A8.1 Malware Protection **Are all of your desktop computers, laptops, tablets and mobile phones protected from malware by either:** **A - Having anti-malware software installed** **and/or** **B - Limiting installation of applications by application allow listing (For example, using an app store and a list of approved applications, using a Mobile Device Management(MDM solution)** **or** **C - None of the above, please describe** Please select all the options that are in use in your organisation across all your devices. Most organisations that use smartphones and standard laptops will need to select both option A and B. Option A - option for all in-scope devices running Windows or macOS including servers, desktop computers; laptop computers Option B - option for all in-scope devices Option C - none of the above, explanation notes will be required.	0: A - Anti-Malware Software	Compliant
A8.2 Daily Update **If Option A has been selected: Where you have anti-malware software installed,**	Yes Custom Fields: Applicant Notes:	Compliant

is it set to update in line with the vendor's guidelines and prevent malware from running on detection? *This is usually the default setting for anti-malware software. You can check these settings in the configuration screen for your anti-malware software. You can use any commonly used anti-malware product, whether free or paid-for as long as it can meet the requirements in this question. For the avoidance of doubt, Windows Defender is suitable for this purpose.*	Malwarebytes endpoint detection and response (EDR) Cloud managed which updates itself and protects the staff from malware / malicious websites and takes preventive actions against a possible threat. 1) Create Daily Software Inventory Scans, Daily Threat Scans and Weekly Custom Scans (IR) 2) Exclude your software applications from being flagged or monitored (IR) 3) Turn off Scan for rootkits (IR) 4) Turn on Tamper protection (IR) 5) For servers, change a few endpoint agent settings (EP) 6) Keep protection settings enabled (EP) 7) Enable Brute Force Protection (EP) 8) Toggle on Flight Recorder to enable endpoint data storage for threat investigation (EDR) 9) Enable Advanced settings for Suspicious Activity Monitoring 10) Enable Ransomware Rollback (EDR)	
A8.3 Scan Web Pages **If Option A has been selected: Where you have anti-malware software installed, is it set to scan web pages you visit and warn you about accessing malicious websites?** *Your anti-malware software or internet browser should be configured to prevent access to known malicious websites. On Windows 10, SmartScreen can provide this functionality.*	Yes Custom Fields: Applicant Notes: Malwarebytes endpoint detection and response (EDR) protects uses from malware / virus when visiting websites and blocks the website from loading and also logs the user / website that was being visited which will be reviewed and reported back to the Directors	Compliant
Acceptance Please read these terms and conditions carefully. Do you agree to these terms? NOTE: if you do not agree to these terms, your answers will not be assessed or certified.	I accept	Compliant
All Answers Approved Have all the answers provided in this assessment been approved at Board level or equivalent? An appropriate person will be asked to validate your answers when you submit your questions.	Yes Custom Fields: Applicant Notes: Robert the director has seen the answers and happy with the submit questions	Compliant