Cyber Essentials Scheme

Validated by: Ian Vernon, CIIO

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 (Montpellier) scheme. Your certificate number is **07641a09-5b66-4c54-91df-4a8a2688d06f** and can be found here:

https://registry.blockmarktech.com/certificates/07641a09-5b66-4c54-91df-4a8a2688d06f/

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.	AWTG 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.	05793772	Compliant

A1.4 Organisation Address What is your organisation's address? Please provide the legal registered address for your organisation, if different from the main operating location.	UK Custom Fields: Address Line 1: 8 Canham Mews Address Line 2: Canham Road Town/City: London County: London Postcode: W3 7SR Country: United Kingdom	Compliant
A1.5 Organisation Occupation **What is your main business?** *Please summarise the main occupation of your organisation.*	Telecoms Custom Fields: Applicant Notes: 61200 - Wireless Telecommunications activities	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.awtg.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".*	Renewal	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: Secondary Reason: To Generally Improve Our Security	Compliant

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).*	London	Compliant

A2.4 End User Devices Please list the quantities and operating 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.*	1 x MacBook laptop running macOS - Version 14.4 1 x MacBook laptop running macOS - Version 14.1.2 47 x Windows laptops running Windows 11 Professional Version 22H2 OS Build 22621.3155	Compliant
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 (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*	None	Compliant

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*	5 x Dell Servers running Linux Ubuntu 22.04 1 x Dell Server running 20.04 LTS	Compliant
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. A 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.*	Working mobiles: 1 x Samsung GalaxyS24 - Android 14 1 x iPhone 15 pro Max- IOS 17.3.1	Compliant

A2.7 Networks	Main Network at Head London Office, this network is comprised of three networks. One to allow corporate internet, One for Corporate Voice, One for Guest. All other functions cloud based	Compliant
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*		
A2.7.1 Home Workers	0	Compliant
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*		

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.* *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.*	2 x Fortigate 100F Firewalls 3 x Cisco CBS 350 24 10G layer 3 switches, 1 x Cisco CBS 350 24 1G PoE layer 3 switches, 2 x Ruckus R650 Unleashed WAPs	Compliant
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 Azure for office 365 solutions IONOS cloud for the web site hosting (awtg.co.uk) Google Cloud for hosting solutions	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.*	Ian Vernon Custom Fields: Responsible Person Role: CIIO	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 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/*	Opt-Out	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: Corporate network is segmented from external networks by firewall. Internal networks are zoned by access by firewall.	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 system of their device.	Virtual firewall restrictions are in place when a managed device is on an external network. Corporate PCs use VPN to connect to onprem corporate assets when off-site.	Compliant

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: Unique passwords are generate by password manager for all devices.	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.*	MOC is raised to cover the change. New random password is generated and password is changed on device	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 Requirements for IT Infrastructure' document.* https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf	0: A. Multi-factor authentication with a minimum password length of 8 characters and no maximum length, 1: C. A password minimum length of 12 characters and no maximum length	Compliant
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: Network device passwords are changed by default on any suspected instance as a first task.	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: VPN service hosted on firewall.For access to legacy voice services	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: This requirement is for external access to protected services for key individuals and engineers.	Compliant
A4.6 Firewall Service Process **If you do have services enabled on your firewall, do you have a process to ensure 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?).*	yes as per company security policy; reviews are held every 3 months	Compliant
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: All services are blocked as default.	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: Configuration of boundary devices are only permitted from internal management network	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 firewalls are configured on all dktops and servers	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).*	All laptops that are company supplied are wiped and installed with the company image. All devices not compatible with the company image have only essential services enabled.Policies are in place to prevent end users from changing enforced policies	Compliant

A5.2 Remove Unrequired User Accounts	Yes	Compliant
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""*	Custom Fields: Applicant Notes: Only users with a verified company account can be established on end user devices.	
A5.3 Change Default Password	Yes	Compliant
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".*	Custom Fields: Applicant Notes: Default passwords are randomised and changed. Default account name is also randomised per device.	
A5.4 Internally Hosted External Services	Yes	Compliant
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.*	Custom Fields: Applicant Notes: VPN services are provided to some key internal users.	

A5.5 External Service Password Configuration **If yes to question A5.4, which option of password-based authentication do you use?** **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 section about 'Password-based 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	0: A. Multi-factor authentication with a minimum password length of 8 characters and no maximum length, 1: B. Automatic blocking of common passwords, with a minimum password length of 8 characters and no maximum length	Compliant
A5.6 Compromised Password on External Service **Describe the process in place for changing passwords on your external services when you believe they have 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 know how to change the password if this occurs.*	Passwords are blocked on compromise or suspected compromise. Passwords can then be changed via the management console by the administrator. End Users may change their password by self-service portal after authentication with the associated MFA.	Compliant
A5.7 External Service Brute Force **When not using multi-factor authentication, which option are you using to protect your external service from brute force attacks?** **A. Throttling the rate of attempts** **B. Locking accounts after 10 unsuccessful attempts** **C. None of the above, please describe** *The external service that you provide must be set to slow down or stop attempts to log in if the wrong username and password have been tried a number of times. This reduces the opportunity for cyber criminals to keep trying different passwords (brute-forcing) in the hope of gaining access.*	B. Locking accounts after 10 unsuccessful attempts Custom Fields: Applicant Notes: Using multi-factor authentication. Accounts locked after 5 unsuccessful attempts	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	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: Devices have biometric devices, finger print or face id. Yubi keys are also used.	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 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.	Biometric Test where credentials are used to solely access device	Compliant

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 devices run latest release of windows 11 or macos. Smartphones have the latest vendor android / iOS deployed.	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 used on devces is under support by vendor.	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.*	Windows devices use Edge - packaged and updated by Version 126.0.2592.87 Mac devices Safari - Packaged and updated by Apple Version 17.5 IOS devices - Safari packaged and updated by Apple 17.5	Compliant

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.*	All Windows devices use latest version of Windows Defender and Bitdefender end point security tools (the latest version: 7.9.13.423 released in 27.06.24) Mac OS latest version of Bitdefender updated from bitdefender central portal Agent Type: BEST Product version: 7.16.44.200006	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.*	Outlook 365. Online or desktop app is the only approved email application. Latest version is used.	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.*	MS365 Online MS365 Desktop Apps	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 software licenses are procured through the software manufacture and are either per seat global licenses or assigned directly to end users.	Compliant

A6.4 Security Updates - Operating 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.*	Yes Custom Fields: Applicant Notes: Security updates are installed within 14 days after canary testing on sandbox machines.	Compliant
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 Custom Fields: Applicant Notes: Windows/IOS/Androd/MacOS and Office apps apply the latest updates automatically Ubuntu Linux auto updates security patches	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.*	Typically software vendors that do not provide auto updates notify of updates by email Vendor support sites are regularly checked for packages every 7 days (Friday) Any notified or discovered update or patch is then assessed and deployed.	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.* *You are not required to install feature updates or optional updates in order to meet this requirement, just high-risk or critical security updates.*	Yes Custom Fields: Applicant Notes: All high-risk or critical updates are assed and deployed as a priority	Compliant
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 Custom Fields: Applicant Notes: Where this functionality is provided by the vendor auto update is enabled as per policy.	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.*	Where auto updates are not available, discovered or notified updates are eithe manually installed on each effected device or packaged and issued by policy server to end user devices. Updates checked every 7 days on Friday	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: Yes out of date software and frameworks are regularly removed. when no longer needed to support software packages.	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.* *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.*	Unsupported software is not permitted to be used.	Compliant
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.*	User access is based on Role based access. Role is defined by job description and job requirements as documented. Account approval is granted by Department Manager + HR + CIIO	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 Custom Fields: Applicant Notes: All acounts both admin and non admin must be unique. Shared accounts are not permitted.	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.*	HR offboarding process is followed. Offboarding process has an interface with IT to ensure that all IT access is removed and devices returned	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.*	Staff are given access based on thier role. Roles are regularly reviewed by HR and management and access assed and updated if required. If a user changes role then the HR process has an interface to notify IT of the change of role.	Compliant
A7.5 Administrator Approval **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.*	Process is documented and recorded and any administrative access requires management and HR approval.	Compliant
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.*	admin functions require a seperate admin account. Admin account are restricted where possible from performing day to day tasks. e.g. admin accounts are unable to browse internet.	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.*	admin account permissions are controlled and enforced by domain policy	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: All admin account assignment is documented All admin account usage is logged and reported for audit purposes	Compliant
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: ISO 27001 process and HR processes both mandate regular access rights review.	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*	Accounts are temporarily blocked after initial 3 failed attempts Block time is randomised and requires a back off period Accounts will be disabled after multiple blocked periods. Usuall 3 but may be soon depending on system analytics.	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 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*	system policy mandates password complexity and the rescue of existing passwords plus the blocking of common or easy to guess passwords. Policy is enforced automatically. Using multi-factor authentication The password requirements are: -Minimum length:8 -Maximum length:40 -Characters Required: At least one capital letter, at least one symbol, at least one number	Compliant

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*	Company IT handbook explains certain strategies users may use to generate a password. Password change prompt has a pop up that explains and shows examples Password change prompt will give a visual traffic light as to the quality of the chosen password and will suggest user tries again if not secure enough All staff undergo CBT training for security which details strategies on how to choose and secure passwords. Users are trained and provided with personal spaceCompany IT handbook explains certain strategies users may use to generate a password. Password change prompt has a pop up that explains and shows examples Password change prompt will give a visual traffic light as to the quality of the chosen password and will suggest user tries again if not secure enough All staff undergo CBT training for security which details strategies on how to choose and secure passwords. Users are trained and provided with personal space on corporate password safe to securely store passwords.	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: Yes policy documents how to report a suspected coprmimsed password, how to request account be blocked. Policy also documents how user can change their password on the self service portal if they are able to.	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 service to provide MFA. Examples of cloud services that can be linked to are Azure, MS365, Google Workspace.*	Yes Custom Fields: Applicant Notes: all services require the use of MFA. either SMS Authenticator APP Yubikey	Compliant

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: All accounts both admin and non admin must have MFA	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 Custom Fields: Applicant Notes: yes all accounts must have MFA	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, 1: B - Limiting installation of applications by application allow listing from an approved app store	Compliant

A8.2 Daily Update **If Option A has been selected: Where you have anti-malware software installed, 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.*	Yes Custom Fields: Applicant Notes: all anti malware updates when vendor releases new patches	Compliant
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: Yes browaser traffic light extension is provided to visually indicate to end user the security score for website	Compliant
A8.4 Application Signing **If Option B has been selected: Where you use an app-store or application signing, are users restricted from installing unsigned applications?** *Some operating systems which include Windows S, Chromebooks, mobile phones and tablets restrict you from installing unsigned applications. Usually you have to "root" or "jailbreak" a device to allow unsigned applications.*	Yes	Compliant

A8.5 Approved Application List **If Option B has been selected: Where you use an app-store or application signing, do you ensure that users only install applications that have been approved by your organisation and do you maintain this list of approved applications?** *You must create a list of approved applications and ensure users only install these applications on their devices. This includes employee-owned devices. You may use mobile device management (MDM) software to meet this requirement but you are not required to use MDM software if you can meet the requirements using good policy, processes and training of staff.*	Yes Custom Fields: Applicant Notes: Approved list of applications are documented. Users must request permission to install software on company devices	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	Compliant