Cyber Essentials Scheme

Report date: 1/3/2024
Applicant: NQA Certification Ltd (CE 2024),

Validated by: S Croxford, IT Manager

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 **d065ecaa-8ab3-460b-95f3-cbdcd9291394** and can be found here:

https://registry.blockmarktech.com/certificates/d065ecaa-8ab3-460b-95f3-cbdcd9291394/

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.	NQA Certification 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.	09351758	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: Address Line 1: Warwick House Address Line 2: Houghton Hall Park Town/City: Houghton Regis County: Bedfordshire Postcode: LU5 5ZX Country: United Kingdom	
A1.5 Organisation Occupation **What is your main business?** *Please summarise the main occupation of your organisation.*	Other (please describe) Custom Fields: Applicant Notes: NQA is a UKAS Accredited Certification Body.	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.nqa.com/en-gb	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 Generally Improve Our Security Custom Fields: Secondary Reason: Other Applicant Notes: We certify others businesses for ISO 27001, cyber essentials help us demonstrate that we take security seriously as an organisation.	Compliant
A1.8.5 Other Reason **What are the reasons you have applied for the certification which you described as "other"?**	Cyber Essentials certification supports NQAs trusted brand reputation and acts in part as a measure of our cyber security.	Compliant

Please provide a description.		
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.*	No Custom Fields: Applicant Notes: NQA UK Operations only.	Compliant
A2.2 Scope Description **If you are not certifying your whole organisation, then what scope description would you like to appear on your certificate and website?** *Your scope description should provide details of any areas of your business that have internet access and have been excluded from the assessment.* *You will need to have a clear excluding statement within your scope description, for example, "whole organisation excluding development network".*	NQA UK operational site only, sole office located in Dunstable.	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).*	The office for NQA UK Ltd as detailed in previous section.	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.*	We have 120 HP laptops running Windows 10 Pro 22H2.	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***	Not Applicable.	Compliant

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*	2 x VMware ESXi 7.0.3 hosts running virtual machines; 5 x Windows 2016 (covered by Extended Security Updates) 1 x Windows 2012 R2 (which is covered by Extended Security Updates until it is upgraded later this year) 1 x Windows 2019 (covered by Extended Security Updates)	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.*	4 x iPhone 8 iOS 16 42 x iPhone SE (2nd Gen.) iOS 16 25 x iPhone SE (3rd Gen.) iOS 17 13 x iPhone 7 iOS 15 1 x Samsung A34 G5 Android V. 14	Compliant
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,*	Main office Lan and wireless at Dunstable head office used by NQA Employees. Guest wireless at Dunstable used by visitors.	Compliant

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 **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*	59 Contracted home workers at time of assessment.	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.* *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 Cisco 4331 Integrated Services Router/K9 running version 17.6 1 x VMWare SD-WAN Edge 510N	Compliant
A2.9 Cloud Services Please list all of your cloud services that are in use by your organisation and	Microsoft - Office 365, Exchange, Azure, OneDrive ADP - Payroll services Breathe - HR services portal	Compliant

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	Adobe - document signing service	
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.*	Laura Fletcher. Custom Fields: Responsible Person Role: Managing Director.	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	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.	All devices are corporate owned, we do not operate BYOD. Fieldbased/Home-based workers use Windows VPN client to connect office systems.	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?**	Yes	Compliant

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.*		
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.*	Initial admin credentials are changed immediately using the process as follows; a Password reset is achieved by Remote Login using SSH Putty.exe , the Factory Default Login are used to Firewall interface -System Administration confirmed Password updated Confirm New password.	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: B. Automatic blocking of common passwords, with a minimum password length of 8 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?**	Yes	Compliant

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.*		
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.*	No Custom Fields: Applicant Notes: No, as a company, we do not provide/require any services that is accessible from internet for which we do not have a documented business case. The only service we provide are online training courses that are hosted on 3rd party.	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: We do not have any services that are required to be advertised to the internet. The firewall settings have been configured, checked & pen tested to ensure all services are blocked to ensure they are not advertised to the internet.	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"*	Yes Custom Fields: Applicant Notes: Network admin & enterprise Manager use At&T private VPN connection SSH to connect to routers and firewalls. Management of devices is restricted to trusted IP addresses.	Compliant

to this question.		
A4.9 Documented Admin Access **If you answered yes in question A4.8, is there a documented business requirement for this access?** *When you have made a decision to provide external access to your routers and firewalls, this decision must be documented (for example, written down).*	Yes Custom Fields: Applicant Notes: Only two administrators have access to these routers & firewalls. These are Network administrator and Enterprise Manager. NQA Access Document outlines these requirements with criteria.	Compliant
A4.10 Admin Access Method **If you answered yes in question A4.8, is the access to your firewall settings protected by either multi-factor authentication or by only allowing trusted IP addresses combined with managed authentication to access the settings?** *If you allow direct access to configuration settings via your router or firewall's external interface, this must be protected by one of the two options.* *Please explain which option is used.*	Access to the settings is protected by only allowing trusted IP addresses.	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: Windows Firewall enabled.	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*	Yes, software not on the approved software list is removed in line with the policy using Microsoft InTune. Mobile devices are managed using Cisco Meraki Mobile Manager (MDM).	Compliant

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).*		
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: All NQA hardware are allocated to use only the main User Accounts or IT Admin Accounts for troubleshooting.	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: All User accounts are configured to change passwords every 90 days. NQA password policy outlines the minimum criteria a selective password should meet for usage. Every new account is set with a unique inital password which must be changed upon first login.	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*	Yes Custom Fields: Applicant Notes: We run NQA EQM Management software that requires secure authentication to access and has selective access criteria allocated to users such as IP allowlist.	Compliant

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.		
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: B. Automatic blocking of common passwords, with a minimum password length of 8 characters and no maximum length Custom Fields: Applicant Notes: 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.*	If users believe that their password or account is compromised, or if the security team notice a suspicious login attempt, an immediate action is taken. The incident is recorded on the ticketing system. Account is locked until user has changed their password.	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**	B. Locking accounts after 10 unsuccessful attempts Custom Fields: Applicant Notes: The Azure/Active Directory policies are designed to ensure accounts are locked out after 3 unsuccessful attempts.	Compliant Assessor Notes: User has described controls more strict than what IASME requires, this answer is compliant.

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.		
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: Auto-run or auto play are disabled via group policy and InTune. In addition, USB-Lock-RP centralised USB management software is used to prevent unauthorised removeable media from being used on company devices.	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: Endpoints auto-lock after 5 minutes of inactivity.	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.	Group Policy setting enforces device locking with minimum password length of 8 characters supported by a deny list.	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 OS and firmware are within support and receive security updates.	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	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 v122.0.6261.70 Edge v122.0.2365.52	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.*	Microsoft Defender v.4.18.23110.3 with Antivirus Version: 1.405.671.0	Compliant

For example: Sophos Endpoint Protection V10, Windows Defender, Bitdefender Internet Security 2020.		
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.*	Microsoft Outlook for Microsoft 365 MSO (Version 2401 Build 16.0.17231.20236) 64-bit	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.*	Microsoft 365 Apps for Enterprise Version 2401 Build 16.0.17231.20236 64-bit	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 is licensed and updated as per the publishers recommendations. Our Licensing Team manages all our standard software licenses.	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*	Yes Custom Fields: Applicant Notes: Patches for OS are applied via Microsoft InTune. Critical firmware is applied in line with the IT Policy within 14 days by the network administrator. iOS devices are required to be updated within 14 days for critical and high-risk updates. Non-complying iOS devices are isolated using MDM until updates applied. Non-compliant iOS devices with missing	Compliant

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.*	critical or high-risk updates will be manually isolated from network access within 14 days by IT Support Specialist following amended IT Security Policy. The policy requires regular monitoring of newly released iOS critical and high-risk updates.	
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.*	Updates are applied automatically.	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: These are applied via Microsoft Intune.	Compliant
A6.5.1 Auto-Updates - Applications **Are all updates applied on your applications by enabling auto updates?**	Yes	Compliant

Most devices have the option to enable auto updates. Auto updates should be enabled where possible.		
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.*	Not applicable as auto updates are enabled. See previous question 6.5.1.	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	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.*	Not applicable as unsupported software is either updated so it is supported or removed via Intune.	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.*	Yes. User Account request is sent by HR manager or Senior management to IT services. IT Tickets are generated and a digitally signed NUR FORM (New User Request form) is issued to IT Services. The account profile is approved by relevant authorities such as HR. The user account is then created as per role. Accounts are then created in Active Directory and Exchange online, and the permissions are then granted as per the NUR form.	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: Yes. Access is controlled by Active Directory/Azure authentication which contains a list of criteria such as unique user name and password required.	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.*	A leaver is reported by HR manager or senior management to IT services. An IT ticket is generated and NUT FORM (NQA User termination Form) is issued by IT services for the Requester to approved the Users date & time of leaving and includes the Hardware to be returned. (With Reference to NUT process document) User and Computer accounts are then disabled, as are remote access rights, e.g. VPN access.	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.*	Yes, user access to share drives and shared mailboxes is defined by Active Directory/Exchange Security groups. The request is sent to IT Services, by relevant authorities in Management, and recorded in Ticketing System. Changes are made and tickets are closed. The requester gets the notification and the description of the actions taken.	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*	Yes. In line with the policy, all access for administrator access is granted only via a written request to IT. From there the IT Director or Enterprise Administrator reviews the request and approves or denies the request. If approved, the enterprise administrator creates the account. If denied, the reason is provided back to the person who made the request.	Compliant

organisation.		
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.*	Normal users do not have administrator access. Anyone who needs administrator access has a separate admin account and IT policy prohibits using this as a regular user 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.*	Admin accounts do not have mailboxes and web browsing is prohibited via IT Policy. This ensures those with admin accounts do not use those accounts for everyday use. Standard accounts are used for normal day-to-day tasks. The admin accounts are only used where necessary. Staff training is also provided in regards to administrator accounts and when to use them.	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: A list is maintained by the enterprise admin and is reviewed on a regular basis.	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*	Yes Custom Fields: Applicant Notes: A list is maintained by the enterprise administrator and is reviewed on a regualar basis.	Compliant

be monthly, quarterly or annually. Any users who no longer need administrative access to carry out their role should have it removed.		
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*	Account locked out until investigated by security team after 3 unsuccessful attempts within 1 minute.	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*	Passwords must meet these complexity requirements; Password must contain min. 8 (no maximum) characters from at least three of the following categories: 1. Uppercase letters 2. Lowercase letters 3. Base 10 digits (0 through 9) 4. Non-alphanumeric characters (special characters) 5. Any Unicode character thats categorized as an alphabetic character but isnt uppercase or lowercase. These requirements are enforced with Azure and Active Directory policies.	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*	Advice given upon starting employment at IT induction. Traning also takes place for entire organisation. Additionally, users encouraged to use secure password generators, such as https://bitwarden.com/password-generator/.	Compliant

Infrastructure document. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf		
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: There is a documented password policy and a procedure for resetting the password when an account is believed to have been compromised. This procedure forces a password change on the user in question.	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	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	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, 1: B - Limiting installation of applications by application allow listing from an approved app store Custom Fields: Applicant Notes: Endpoint (Windows) devices are protected via Microsoft Defender for Endpoint. Mobile devices and their apps are controlled by IT Acceptable Use Policy and monitored by routine report analysis of MDM (Meraki) software inventory.	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: As default.	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	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	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