Cyber Essentials Scheme

Report date: 25/7/2025
Applicant: NetFM UK Ltd,

Validation Attached
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 (Willow) scheme. Your certificate number is **c468ba8d-08f3-4ab0-aae3-b2169bc6435c** and can be found here:

https://registry.blockmarktech.com/certificates/c468ba8d-08f3-4ab0-aae3-b2169bc6435c/

Your insurance number is 0038253756 and it can be found here:

https://registry.blockmarktech.com/certificates/ed85b931-a8a5-428e-9810-3b3af809c73c/
The insurance certificate has been set to private, but can be viewed when
you register / log-in appropriately. We recommend keeping a hard copy or
separate copy of your insurance certificate / schedule in case you need
to make a claim and are unable to access your electronic copy. Both
your Cyber Essentials and Insurance certificates have been emailed to
you in separate messages as pdf attachments.

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

Applicant Answers

	Applicant Answers	Assessor Score
A1.1 Organisation Name? What is your organisation's name? The answer given in A1.1 is the name that will be displayed on your certificate and has a character limit of 150 including spaces. Where 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.	NetFM UK Ltd	Compliant
A1.2 Organisation Type What type of organisation are you? “LTD” – Limited Company (Ltd or PLC) “LLP” – Limited Liability Partnership (LLP) “CIC” – Community Interest Company (CIC) “COP” – Cooperative “MTL” – Other Registered Mutual (Community Benefit Society, Credit Union, Building Society, Friendly Society) “CHA” – Registered Charity “GOV” – Government Agency or Public Body “SOL” – Sole Trader “PRT” – Other Partnership “SOC” – Other Club/ Society “OTH” – Other Organisation	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 DUNS number.	08165293	Compliant
A1.4 Organisation Address What is your organisation's address? Please provide the legal registered address for your organisation.	UK Custom Fields: Address Line 1: Withycombe Address Line 2: 45 Church Road East Town/City: Crowthorne County: Berkshire Postcode: RG45 7ND Country: United Kingdom	Compliant
A1.5 Organisation Occupation What is your main business? Please summarise the main occupation of your organisation.	IT Custom Fields: Applicant Notes: Software Development	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.	https : / / visitor . express	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 Custom Fields: Applicant Notes: Required for Cyber Essentials Plus	Compliant
A1.8 Reasons 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. Cyber Essentials Requirements for IT Infrastructure v3.2	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.	No	Compliant

A1.11 Contact Permission Can IASME contact you for research purposes? Both IASME and the UK government occasionally need to ask questions about the process and/or benefits of the Cyber Essentials scheme for research purposes. If you agree to this we will contact you via the email address you registered with, you are free to not respond if we do contact you.	No	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 opt in to the included insurance. Your whole organisation includes all divisions, people and devices which access your organisation's data and services. About Scope Subset Scoping Guidance	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 (e.g. All UK offices) or simply list the locations in scope (e.g. Manchester and Glasgow retail stores).	No central office location - all homeworkers with access to data centre servers hosted in London with OVH	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 you 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 22H2 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. **Extended Security Update schemes** For any end-of-life operating system that has an extended security update program, you must maintain the required subscription. If you are using Windows 10 beyond the 14th October 2025 you must be signed up to the Microsoft Extended Security Update program in order to remain compliant. Further guidance: Operating System Support Guidance to BYOD	3x MacBook Air Laptop running macOS 15 Sequoia 1x Intel Nuc running Ubuntu 24 . 04	Compliant

A2.4.1 Thin Client Devices Please list the quantity of thin clients within the 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 'Cyber Essentials Requirements for IT 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 to be supported and receiving security updates. Cyber Essentials Requirements for IT Infrastructure v3.2	None	Compliant
A2.5 Server Devices Please list the quantity of servers, virtual servers, virtual server hosts (hypervisors) and Virtual Desktop Infrastructure (VDI) servers. You must include the operating system. Please list the quantity of all servers within the 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 Red Hat Enterprise Linux 8.3	2x Ubuntu running Ubuntu 24 . 04 Noble Numbat (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 within the scope of the certification only require the make and operating system to be listed. Devices that are connecting to cloud services must be included. A scope that does not include end user devices is not acceptable. Guidance to BYOD Operating System Support	1x Apple iPhone 13 running iOS 18 1x Apple iPhone 16 Pro running iOS 18 1x Pixel 6 running Android 16 Baklava 1x Apple iPhone 16 running iOS 18	Compliant
A2.7 Networks Please provide a list of networks that will be in scope for this assessment. You should include details of each network used in your organisation including its name, location and its purpose (e.g. Main Network at Head Office for administrative use, Development Network at Malvern Office for testing software). You do not need to provide IP addresses or other technical information.	Server network at OVH London - dedicated servers and dedicated edge network firewall . Home workers network - based UK : Crowthorne - Dave . Camberley - Nici . Cambridge - Finlay . Dorset - Toby . We do not provide routers or any access equipment - just the computer device (Mac book or Intel Nuc) . The responsibility lies with the homeworker to apply an OS based firewall on their device and configure rules that allow only external access to the GitLab service and web servers provided by NetFM .	Compliant
A2.7.1 Home or remote workers How many staff are home or remote workers? Any employee that has been given permission to work remotely (for any period of time at the time of the assessment) needs to be classed as a home/remote worker for Cyber Essentials. For further guidance see the Home and remote working section in the Cyber Essentials Requirements for IT Infrastructure document. Cyber Essentials Requirements for IT Infrastructure v3.2	4 Home Workers	Compliant

A2.8 Network Equipment Please provide a list of 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 to and from the internet. 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 have home and/or remote workers they will be relying on software firewalls, please describe in the notes field. You are not required to list any IP addresses, MAC addresses or serial numbers.	No office provided . The edge firewall at OVH is a service provided by OVH . This acts as a boundary for all homeworkers when accessing the OVH servers .	Compliant
A2.9 Cloud Services Please list all of the cloud services that are in use by your organisation and provided by a third party. **Please note that cloud services cannot be excluded from the scope of Cyber Essentials.** You need to include details of all of your cloud services. This includes all types of services - Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Definitions of the different types of cloud services are provided in the 'Cyber Essentials Requirements for IT Infrastructure' document. Cyber Essentials Requirements for IT Infrastructure v3.2	There are 3 could services in use : OVH Dedicated server centre servers GitLab Source code control Security scanning on source code Automated deployments and testing prior Google Full Workplace suite Gmail + Google docs + 2FA for all devices	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.	David Herring Custom Fields: Responsible Person Role: Founder	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-In	Compliant
A3.3 Insurance Contact What is the organisation email contact for the insurance documents? You only need to answer this question if you are taking the insurance. The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification and they will use this to contact you with your insurance documents and renewal information.	nici @ netfm . org	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. **CE Requirement:** You must protect every device in scope with a correctly configured firewall (or network device with firewall functionality). Further guidance: Firewalls	Yes Custom Fields: Applicant Notes: This is managed and rules created purely by OVH . We can add tickets to make changes .	Compliant

A4.1.1 Off Network Firewalls Do you have software firewalls enabled on all of your computers, laptops and servers? Your software firewall needs to be configured and enabled at all times, even when sitting behind a physical/virtual boundary firewall in an office location. Guidance on how to check your software firewall can be found here: About Firewalls **CE Requirement:** You must protect every device in scope with a correctly configured firewall (or network device with firewall functionality). **CE Requirement:** Make sure you use a software firewall on devices which are used on untrusted networks, such as public wifi hotspots. If your organisation doesn't control the network to which a device connects, you must configure a software firewall on the device.	Yes	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 administrator password must be changed on all routers and firewalls, including those that come with a unique password pre-configured (e.g. 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. **CE Requirement:** Change default administrative passwords to a strong and unique password – or disable remote administrative access entirely. Further guidance: About Routers	Yes Custom Fields: Applicant Notes: This is done as part of our standard server setup process .	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.	The data centre firewall has no password set or maintained by us . It can only be set by admin access to the OVH portal which requires 2FA . The password for this account is subject to strict rules : - 10 characters Upper case and lower case mix Must contain number (s) Must contain a special character Only once you have logged in can you access the firewall rules and logs - there is no setting of a password on the OVH edge of network device - it is part of the supplied infrastructure of OVH .	Compliant

A4.3 Firewall Password Configuration How is your firewall password configured? Please select the options being used: A. Multi-factor authentication, with a minimum password length 8 characters and no maximum length B. Automatic blocking of common passwords, with a minimum password length 8 characters and no maximum length C. A password minimum length of 12 characters and no maximum length D. Passwordless system is being used as an alternative to user name and password, please describe E. 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. Cyber Essentials Requirements for IT Infrastructure v3.2 **CE Requirement:** Prevent access to the administrative interface (used to manage firewall configuration) from the internet, unless there is a clear and documented business need, and the interface is protected by one of the following controls: • multi-factor authentication • an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach Further guidance : Bulletproof your passwords	0: A. Multi-factor authentication, with a minimum password length 8 characters and no maximum length Custom Fields: Applicant Notes: We use Bitwarden to generate security strong passwords . We use google multi factor auth for two factor login using google based accounts .	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. **CE Requirement:** You should make sure there is an established process in place to change passwords promptly if you know or suspect a password or account has been compromised. Further guidance: Compromised Accounts	Yes Custom Fields: Applicant Notes: Our firewall password is an ssh - keygen public / private key pair . So no password access is allowed to servers or the UFW software than runs on them .	Compliant
A4.5 Firewall Management Process Do you have a process to manage your 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.	Yes Custom Fields: Applicant Notes: We run dedicated open shh services to allow ssh access for server maintenance . This is only available using ssh private keys - so NO password login is allowed on servers . We also maintain a list of trusted IPs for this server level access .	Compliant

A4.6 Firewall Review Process Have you reviewed your firewall rules in the last 12 months? Please describe your review process. 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?). **CE Requirement:** Remove or disable inbound firewall rules quickly when they are no longer needed.	All incoming connections are disabled on home devices . Only HTTPS and SSH services are enabled on dedicated servers . We do not allow the adding of additional services . Any removals form part of a review process . No additional services have been added to the OVH edge firewall . To modify the existing services on the firewall service you must : - Access the OVH web - portal for control of all services provided . This is via dedicated administrator username / password and 2FA to mobile phone . Once logged into the portal , their are 20 rules for the edge firewall that can be modified - list of IPs that can use this service + port for the service . ie a typical high level firewall rules based list .	Compliant
A4.7 Firewall Inbound Connections Is your firewall configured to allow unauthenticated inbound connections? By default, most firewalls block all services inside the network from being accessed from the internet, but you need to check your firewall settings. **CE Requirement:** Block unauthenticated inbound connections by default.	No Custom Fields: Applicant Notes: Only port 443 - SSL web access is generally available on production servers . This is checked regularly in house using nmap , and periodically by client request using a formal pen test .	Compliant
A4.8 Allowed Connections Please describe how you approve and document your allowed inbound connections. The business case should be documented and recorded. A business case must be signed off at board level and associated risks reviewed regularly. 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. **CE Requirement:** Ensure inbound firewall rules are approved and documented by an authorised person, and include the business need in the documentation.	We run dedicated openshh services to allow ssh access for server maintenance . This is only available using ssh private keys - so NO password login is allowed on servers . We also maintain a list of trusted IPs for this server level access . Only port 443 - SSL web access is generally available on production servers . This is checked regularly in - house using nmap , and periodically by client request using a formal pen test . Documented on the NetFM company wiki .	Compliant

A4.9 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. **CE Requirement:** Prevent access to the administrative interface (used to manage firewall configuration) from the internet, unless there is a clear and documented business need, and the interface is protected by one of the following controls: • multi-factor authentication • an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach Guidance on VPNs	No Custom Fields: Applicant Notes: The only access is from within OVH data centre by dedicated staff	Compliant

A5.1 Remove Unused Software Have you removed or disabled 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 achieve this. You must remove or disable 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 installed applications: Windows: Right-click on Start > Apps and Features macOS: Open Finder > Applications Linux: Open your software package manager (apt, rpm, yum) **CE Requirement:** You must regularly remove or disable unnecessary software (including applications, system utilities and network services). Further guidance : Removing unnecessary software	We regularly run Linux apt auto remove after a Tuesday update to ensure only relevant software is installed on the servers . We also use dedicated Docker containers for each micro service within Visitor Express to further enforce this minimal software approach . Homeworker based machines are under the direct control of the homeworker . They are regularly updated by individual developers who are skilled in the software removal on their OS device . We meet up across the entire company twice yearly , and as part of this process will check all homeworkers are running the latest patched version of their OS , and that they have not installed anything that might compromise company wide security by checking list of applications installed .	Compliant
A5.2 Remove Unrequired User Accounts Have you ensured that all your laptops, computers, servers, tablets, mobile devices and cloud services only contain necessary user accounts that are regularly used in the course of your business? You must remove or disable any user accounts that are not needed in day-to-day use on all devices and cloud services. To view user accounts: Windows: Right-click on Start > Computer Management > Users macOS: System Settings > Users and Groups Linux: "cat/etc/passwd" **CE Requirement:** You must regularly remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used).	Yes Custom Fields: Applicant Notes: Personal devices are under the direct control of that homeworker . All employees are provided a central google workplace login for access to company email , documents and GitLab access for source code control . Login on homeworker devices is under the direct control of individual homeworkers .	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". **CE Requirement:** You must regularly change any default or guessable account passwords. Use technical controls to manage the quality of passwords. This will include one of the following: • using multi-factor authentication • a minimum password length of at least 12 characters, with no maximum length restrictions • a minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list	Yes Custom Fields: Applicant Notes: We mandate two factor auth for all backend infrastructure access . We use Bitwarden for strong password generator with shared access across all NetFM devices .	Compliant
A5.4 Internally hosted External Services Do you run or host external services that provide 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 such as a SaaS or PaaS cloud service 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. **CE Requirement:** Ensure users are authenticated before allowing them access to organisational data or services.	Yes	Compliant

A5.5 External services Authentication If yes to question A5.4, which authentication option 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. Passwordless, please describe E. 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. Cyber Essentials Requirements for IT Infrastructure v3.2 **CE Requirement**: Use technical controls to manage the quality of passwords. This will include one of the following: • using multi-factor authentication • a minimum password length of at least 12 characters, with no maximum length restrictions • a minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list	0: A. Multi-factor authentication, with a minimum password length of 8 characters and no maximum length Custom Fields: Applicant Notes: Use Bitwarden to maintain very strong passwords across all services .	Compliant

A5.6 External services password change process 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. **CE Requirement**: You should also make sure there is an established process in place to change passwords promptly if you know or suspect a password or account has been compromised.	We use Bitwarden to generate new passwords . We use google password checker to see if a password has been compromised - checking via google admin controls . To change password : 1 . Access Bitwarden service using 2FA 2 . Select the web service for the password change 3 . Click generate new strong password 4 . Save changes . The password is too complicated to be written down easily and is only available from the Bitwarden vault .	Compliant

A5.7 External services brute-force protection 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. **CE Requirement:** You must protect your chosen authentication method (which can be biometric authentication, password or PIN) against brute-force attacks. When it's possible to configure, you should apply one of the following: • 'throttling' the rate of attempts, so that the length of time the user must wait between attempts increases with each unsuccessful attempt - you shouldn't allow more than 10 guesses in 5 minutes • locking devices after more than 10 unsuccessful attempts • When the vendor doesn't allow you to configure the above, use the vendor's default setting.	0: A. Throttling the rate of attempts	Compliant

A5.8 Auto-run Disabled Have you disabled any feature which allows automatic file execution of downloaded or imported files without user authorisation? 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. **CE Requirement:** Disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded).	Yes Custom Fields: Applicant Notes: Developers use either Linux or Mac based devices .	Compliant
A5.9 Device Unlocking When a device requires a user to have the device in hand, 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. **CE Requirement:** Ensure appropriate device locking controls for users that are physically present.	Yes Custom Fields: Applicant Notes: We use finger print access to development devices .	Compliant

A5.10 Device Unlocking 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. Cyber Essentials Requirements for IT Infrastructure v3.2 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. **CE Requirement:** If a device requires a user's physical presence to access a device's services (such as logging on to a laptop or unlocking a mobile phone), a credential such as a biometric, password or PIN must be in place before a user can gain access to the services. You must protect your chosen authentication method against brute-force attacks. When it's possible to configure, you should apply one of the following: • 'throttling' the rate of attempts, so that the length of time the user must wait between attempts increases with each unsuccessful attempt - you shouldn't allow more than 10 guesses in 5 minutes • locking devices after more than 10 unsuccessful attempts • When the vendor doesn't allow you to configure the above, use the vendor's default setting.	We do not control individual homeworker devices . Training encourages them to set a 2 minute inactivity lock screen with fingerprint reactivation . These are used solely to unlock personal devices and do not provide access to any company servers or company infrastructure .	Compliant

A6.1 Supported Operating System Are all operating systems on your devices supported by a vendor that produces regular security updates and vulnerability fixes? 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 could be any of the following examples: Windows 7/XP/Vista/ Server 2003, macOS Mojave, iOS 12, iOS 13, Android 8 and Ubuntu Linux 17.10. This is not an extensive list and you should always check with the vendor to confirm if an operating system is still supported 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. **CE Requirement**: You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported. Vulnerability fixes include patches, updates, registry fixes, configuration changes, scripts or any other mechanism approved by the vendor to fix a known vulnerability. **Extended Security Update schemes** For any end-of-life operating system that has an extended security update program, you must maintain the required subscription. If you are using Windows 10 beyond the 14th October 2025 you must be signed up to the Microsoft Extended Security Update program in order to remain compliant. Further guidance: Operating System Support Navigating the pitfalls of legacy software	Yes	Compliant

A6.2 Supported software Is all the software on your devices supported by a supplier that produces regular vulnerability fixes for any security problems? All software used by your organisation must be supported by a supplier who provides regular security updates and vulnerability fixes. Unsupported software must be removed from your devices. This includes frameworks and extensions. **CE Requirement:** You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	Yes Custom Fields: Applicant Notes: Ubuntu 24 . 04 . 2 LTS - Long Term Support until April 2027 . We automatically apply all security updates and have an update window of Tuesday 4am - 6am to apply any kernel updates that required a reboot . A message is posted in the clients dedicated WhatsApp support group prior to any updates that require a server reboot . PostgreSQL (v17) - we update directly from the postgres repos on a Tuesday morning . All other Nginx / Uwsgi / Python packages are handled by the standard repos . We use poetry 1 . 8 . 2 to check for Python package conflicts and security of each package . For Visitor Express software (our software) we release updates weekly , and again apply these with prior notice in the Tuesday update window .	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 124, Safari Version 15. **CE Requirement:** You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	Firefox 140 . 0 . 2 Safari v18 . 5 Chrome 138 . 0 . 7204 . 101	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, Microsoft Defender, Bitdefender Internet Security 2023. **CE Requirement:** You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	Mac standard firewall - macOS Sequoiq 15 . 5 For Linux - ClamAV 1 . 4 . 3	Compliant
A6.2.3 Email Applications 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. **CE Requirement:** You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	Google Workplace - Gmail	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. **CE Requirement**: You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	Google Workspace	Compliant

A6.3 Software Licensing Are any of the in-scope software or cloud services unlicensed or unsupported? 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. **CE Requirement:** All software on in-scope devices must be licensed and supported.	No Custom Fields: Applicant Notes: PostgreSQL License , a liberal Open Source license , similar to the BSD or MIT licenses . PostgreSQL Database Management Ubuntu Intellectual property rights policy https : / / ubuntu . com / legal / intellectual - property - policy . Visitor Express End User Agreement NetFM UK Ltd Terms and Conditions https : / / visitor . express / static / pdf / NetFM _ Terms _ And _ Conditions . pdf	Compliant

A6.4 Security Updates - Operating System Are all high-risk or critical security updates and vulnerability fixes for operating systems and router and firewall firmware installed within 14 days of release? You must install all high and critical security updates and vulnerability fixes 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. **CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where: • The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk' • The update addresses vulnerabilities with a CVSSv3 base score of 7 or above • There are no details of the level of vulnerabilities the update fixes provided by the vendor Please note: For optimum security we strongly recommend (but it's not mandatory) that all released updates are applied within 14 days of release. It's important that updates are applied as soon as possible. 14 days is considered a reasonable period to be able to implement this requirement. Any longer would constitute a serious security risk while a shorter period may not be practical.	Yes Custom Fields: Applicant Notes: Use Ubuntu live update service - security patches are immediate . Other updates occur in Tuesday 4am - 6am software update windows	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. **CE Requirement**: All software on in-scope devices must have automatic updates enabled where possible.	Yes Custom Fields: Applicant Notes: Ubuntu live patch	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 and vulnerability fixes 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. **CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where: • The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk' • The update addresses vulnerabilities with a CVSSv3 base score of 7 or above • There are no details of the level of vulnerabilities the update fixes provided by the vendor	We do manual updates on Tuesday mornings 4am to 6am using standard Ubuntu command line tools apt - get update / apt - get upgrade / apt - get dist - upgrade . All updates are applied first the staging service - on separate servers . These are then automated tested using GitLab CI / CD scripts . Once a week we manually login to all servers and check the latest updates have been applied . Sometimes for package like PostgreSQL we use dedicated repos for that software . For the main OS we use the standard Ubuntu based repos . For home based devices we provide training to the end user on how to keep their devices up to date . We do not centrally manage the patching of homeworker devices . We meet up across the entire company twice yearly , and as part of this process will check all homeworkers are running the latest patched version of their OS , and that they have not installed anything that might compromise company wide security by checking list of applications installed .	Compliant

A6.5 Security Updates - Applications Are all high-risk or critical security updates and vulnerability fixes for applications (including any associated files and extensions) installed within 14 days of release? You must install any such updates and vulnerability fixes 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. **CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where: • The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk' • The update addresses vulnerabilities with a CVSSv3 base score of 7 or above • There are no details of the level of vulnerabilities the update fixes provided by the vendor	Yes	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. **CE Requirement:** All software on in-scope devices must have automatic updates enabled where possible.	Yes	Compliant

A6.5.2 Manual Updates - Applications Where auto updates are not being used, how do you ensure all high-risk or critical security updates and vulnerability fixes 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 and vulnerability fixes are applied when auto updates are not configured. If you only use auto updates, please confirm this in the notes field for this question. **CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where: • The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk' • The update addresses vulnerabilities with a CVSSv3 base score of 7 or above • There are no details of the level of vulnerabilities the update fixes provided by the vendor	Two types of application software : - 1 . Our software - Visitor Express . The Visitor Express application is only installed on the OVH servers , and is tightly controlled by GitLab based CICD (continuous integration / continuous delivery) scripts that run immediately on any source code commit . Initial deployment is to staging servers , and once manually checked any commit to master is then deployed to production servers . No Visitor Express software is installed on home worker devices . 2 . Software applications used on home worker machines - chrome + vscode . There are two pieces of application software outside of the OS supplied packages that are deployed on home worker machines . Google Chrome - home workers are educated to regularly click the three dots Help - About Google Chrome - and check for updates . In the dev ops meetings we review what version is installed on home worker devices to ensure the latest updates have been applied . Other OS supplied browsers are maintained up to date by OS updates . If a home worker elects to use Firefox , then the same update manual checking method is applied to this . Home workers mainly use vscode for software development , this has an automatic check for updates on startup , and home workers are educated to click this when it shows updates are available . The same process is also used to update the commonly used extensions to vscode : gitlens + python . Lastly , for commonly used python packages when developing we use poetry to automatically update these as part of the build process . This only runs on the production servers , but ensures the latest fully supported packages are bundled with each build .	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 or vulnerability fixes 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, and all application software. **CE Requirement**: All software on in-scope devices must be removed from devices when it becomes unsupported, or removed from scope by using a defined sub-set that prevents all traffic to/from the internet.	Yes Custom Fields: Applicant Notes: We don t currently use any unsupported software .	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 sub-set 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. Where no unsupported software is used across your whole organisation, please declare this here. **CE Requirement**: All software on in-scope devices must be removed from devices when it becomes unsupported, or removed from scope by using a defined sub-set that prevents all traffic to/from the internet. Further guidance: Subset Scoping Guidance	We don t currently use any unsupported software .	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. **CE Requirement:** Your organisation must have in place a process to create and approve user accounts.	We centrally manage user accounts for company services using Google Workplace . A new user account is only created after they have passed the interviewing process - which includes checking an identification document (passport) . # 1 Google workplace accounts . To create the account : - 1 . Operations directory logs into Google workplace using 2FA . 2 . Creates an email alias firstname . lastname @ netfm . org and email alias firstname @ netfm . org 3 . Sets the gmail workplace account as active and creates a one time only secure password . 4 . Sends email address to the new starter via encrypted business WhatsApp . 5 . Gives password verbally over phone - company policy never to write down a password . A new user can select Linux or Mac for their home device - a single account for them is created on their chosen device as follows : - # 2 Linux account - home device 1 . Install Ubuntu 24 . 04 LTS desktop version 2 . Setup username as first name of the home worker receiving the device 3 . Use a common a three word + date secure password for the account 4 . State to end user that no more accounts can be created on this device - it is purely for company work using the designated account created for them 5 . A separate administrator account is created by operations director - that homeworker does not have access to . # 3 Mac account - home device 1 . Install macOS Sequoia 15 . 5 2 . Setup an account with the first name of the homeworker who will use this device 3 . Use a common a three word + date secure password for the account 4 . State to end user that no more accounts can be created on this device - it is purely for company work using the designated account created for them 5 . A separate administrator account is created by operations director - that homeworker does not have access to . Home devices users are able to change their password - but must adhere to the company policy of using a three word + date password .	Compliant

	They are not allowed to create more accounts on their home device . They are not allowed to use their home device other than for company business using the account that has already been created for them . Server accounts within OVH We have an administration account for the OVH server portal - these accounts are separate from home device and google workplace accounts . They allow dev - ops designated staff to access the backend OVH server portal and backend OVH hosted servers using ssh for administrations . The accounts are 2FA and a designated dev - ops account is created on the OVH portal for each home worker granted dev - ops access : 1 . Login to OVH web portal using 2FA 2 . Click accounts in drop down 3 . Select + to add new account 4 . Create account with same username as the homeworker uses on home device 5 . Create a strong three word + date password for that end user to access OVH 6 . Select 2FA - enter home workers mobile number 7 . Click create account	
A7.2 Unique Credentials Are all your user and administrative accounts accessed by entering unique credentials? You must ensure that no devices, applications or cloud services can be accessed without entering unique access credentials. Accounts must not be shared. **CE Requirement:** Authenticate users with unique credentials before granting access to applications or devices.	Yes	Compliant

A7.3 Leaver 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. **CE Requirement:** Remove or disable user accounts when no longer required.	We manually audit the active accounts - only 4 NetFM staff so easy to do manually . To remove an account from Google workplace : - 1 . Operations directory logs into Google workplace using 2FA . 2 . Removes the email alias firstname . lastname @ netfm . org and email alias firstname @ netfm . org . 3 . Sets the gmail workplace account as inactive . 4 . Sends email company wide to say firstname . lastname @ netfm . org has left company - email is no longer active . If the employee had dev ops access (OVH servers) . 1 . Login to OVH web portal . 2 . select accounts from drop down . 3 . Click on the username to be removed . 4 . Remove account . For the home workers device 1 . Request the home workers device be returned . 2 . Reinstall the homeworkers device with a fresh install account . 3 . set up a test account to check device . 4 . when a new employee starts , create a new account for that employee and remove the test account .	Compliant

A7.4 User Privileges Do you ensure that staff only have the access 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. For Cyber Essentials we require that the principle of least privilege be applied. **CE Requirement**: Your organisation must be in control of your user accounts and the access privileges that allow access to your organisational data and services.	# Google workplace accounts : Manually audit all the 4 accounts in Google workplace - only 4 staff so easy to do manually . To change permissions on an account on google workplace : - 1 . Operations directory logs into Google workplace using 2FA . 2 . Click the email alias firstname . lastname @ netfm . org . 3 . Sets the group memberships according to the access levels employee / reporter / administrator / owner . 4 . Sends company wide email to state permissions have been altered for firstname . lastname @ netfm . org . # Home devices : On home worker devices there is one single login account that does not have administrator access . If a user needs administration level access the device must be manually passed to the operations director to authorise this : # Linux : 1 . login with the company home device administrator account 2 . Add the homeworkers usernames to the group sudo in / etc / groups 3 . Test that homeworker can login and perform administrator commands on device . # Mac : 1 . Login as company home device administrator . 2 . In the System section , click Users & Groups . 3 . To grant a user administrative privileges , click the lock , enter your rootpassword , click your desired user and then select the check box for Allow user to administer this computer . # OVH server accounts : On OVH servers only designated dev - ops employees have accounts created for them on the OVH web portal .	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. **CE Requirement:** Your organisation must have in place a process to create and approve user accounts.	User access levels changes for home devices , Google workplace , and OVH servers has to be submitted via email to the operations director and approved by the company founder before any changes take place . All access levels and accounts are recorded on the company wiki pages so there is a clear knowledge of who has access where . Once approved the changes are made accordingly : For google workplace this is managed directly by the operations director , who can promote or demote a users access level . For OVH server access , the accounts are maintained separately on the OVH web portal and under the direct control of the company founder . For home device changes , once approved these will necessitate the home device being physically passed to the operations director , who can login using the company administrator account for home devices and make the change for the homeworkers account on that device . There is a separate Admin account for home devices to prevent escalation of privileges .	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 using separate accounts. Further guidance : User Access - Just Enough or Just In Time **CE Requirement:** Your organisation must use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks).	We use separate accounts for OVH IaaS administration . These have auto log out on inactivity enabled for 2 minutes . These accounts only exist within the realm of the OVH infrastructure so their use on home based devices is not possible . We do not manage accounts on home based devices . Home based workers (everyone) are educated to not install extract packages on their devices , but administrator access to their home based devices is under their control . When performing administrator access on OVH servers and services home workers use separate google workplace accounts to access the servers with 2FA . These only allow either ssh (terminal login) or web - portal (secure admin interface) access , so no concept of them web browsing / doing other activities on the servers . The servers only run the minimal software to provide their deployment stack . All home workers have separate user and Admin accounts .	Compliant

A7.7 Managing Administrator Account Usage How does your organisation prevent administrator accounts from being used to carry out everyday 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 may not need a technical solution to achieve this, it could be based on good policy, procedure and regular training for staff. **CE Requirement:** Your organisation must use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks).	We do not manage accounts on home based devices . Homeworkers are educated to maintain only the necessary packages on their own devices and are able to talk with operations directory on a Friday dev ops meeting to ensure they get any help on maintaining a secure setup . The home based worker is educated to have a basic user account on their device for access and doing their day to day work , with a separate administrator account that can install packages and perform upgrades on their home based device .	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. **CE Requirement:** Your organisation must have in place a process to create and approve user accounts.	Yes Custom Fields: Applicant Notes: We track all access to the OVH portal for server administration . This is service is provided by OVH login logs , and is maintained by OVH . We track all server activity using standard system accounting built into Ubuntu / Linux - all login attempts are recorded in / var / log / auth . log for both successful and failed logins . Access to Gmail using Google workplace logins is tracked on the Google admin console , showing last login and login history . Gitlab has full login tracking and activity login for each home worker . Lastly , home based workers educated to enable the system accounting software on their device so that at company dev ops meetings they can share their login activity and check only the one account is being used on that device .	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. **CE Requirement:** Your organisation must remove or disable special access privileges when no longer required (when a member of staff changes role, for example).	Yes Custom Fields: Applicant Notes: All home based workers (4 total) are trained and form part of the security team . They are educated to only allow one active secure account on the home worker device , and that this should have administrator access to their home worker device . The 4 local device administrator accounts form part of the company policy . logins to gmail / GitLab our under direct control , of owner and operations director - and controlled by Google workplace . Logins to the OVH infrastructure portal and servers are under direct control of owner and operations director .	Compliant
A7.10 Brute Force Attack Protection Where you have systems that require passwords (or where passwords are a backup for a passwordless system), how are they protected from brute-force attacks? 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' document. Cyber Essentials Requirements for IT Infrastructure v3.2 **CE Requirement**: Passwords are protected against brute-force password guessing by implementing at least one of: • multi-factor authentication • 'throttling' the rate of attempts, so that the length of time the user must wait between attempts increases with each unsuccessful attempt – you shouldn't allow more than 10 guesses in 5 minutes • locking devices after no more than 10 unsuccessful attempts	We have throttling installed on the OVH servers , which allows a maximum of three failed attempts in every 10 minutes . We also have OVH account lock after more than five failed attempts between unsuccessful login . Home based workers are educated to setup auto lockout on their devices as part of the onboarding policy .	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 section about Password-based authentication in the 'Cyber Essentials Requirements for IT Infrastructure' document. Cyber Essentials Requirements for IT Infrastructure v3.2 **CE Requirement**: Use technical controls to manage the quality of passwords. This will include one of the following: • using multi-factor authentication • a minimum password length of at least 12 characters, with no maximum length restrictions • a minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list.	We use Bitwarden to control strong password creation - this ensures a minimum password length of at least 12 characters , with no maximum length restrictions and use automatic blocking of common passwords using a deny list .	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. Cyber Essentials Requirements for IT Infrastructure v3.2 **CE Requirement**: Support users to choose unique passwords for their work accounts by: • educating people about avoiding common passwords, such as a pet's name, common keyboard patterns or passwords they have used elsewhere. This could include teaching people to use the password generator feature built into some password managers • encouraging people to choose longer passwords by promoting the use of multiple words (a minimum of three) to create a password (such as the NCSC's guidance on using three random words) • providing usable secure storage for passwords (for example a password manager or secure locked cabinet) with clear information about how and when it can be used • not enforcing regular password expiry • not enforcing password complexity requirements	We give all users individual accounts for Bitwarden to create strong passwords are always created . Educate home workers to choose longer passwords by promoting the use of multiple (a minimum of three) to create a password , we have promoted examples such as LoveTheSunshine1972 as good exemplar examples for passwords .	Compliant

A7.13 Password Compromise 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. **CE Requirement:** You should make sure there is an established process in place to change passwords promptly if you know or suspect a password or account has been compromised. Further guidance : Compromised accounts	Yes	Compliant
A7.14 Cloud Service MFA 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 this for all users and administrators. For more information see the NCSC's guidance on MFA at Multi-factor authentication for your corporate online services 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. **CE Requirement**: Your organisation must implement MFA, where available – authentication to cloud services must always use MFA. Further guidance : Applying MFA to access cloud services Securing Your Cloud Services	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. **CE Requirement**: Your organisation must implement MFA, where available – authentication to cloud services must always use MFA.	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. **CE Requirement**: Your organisation must implement MFA, where available – authentication to cloud services must always use MFA.	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. **CE Requirement**: You must make sure that a malware protection mechanism is active on all devices in scope. For each device, you must use at least one of the options listed below. • Anti-malware software (option for in-scope devices running Windows or MacOS including servers, desktop computers, laptop computers) • Application allow listing (option for all in-scope devices). Only approved applications, restricted by code signing, are allowed to execute on devices.	0: A - anti-malware software, 1: B - limiting installation of applications by application allow listing from an approved app store	Compliant

A8.2 Anti-malware Updates 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. **CE Requirement**: If you use anti-malware software to protect your device it must be configured to: • be updated in line with vendor recommendations • prevent malware from running • prevent the execution of malicious code	Yes	Compliant
A8.3 Scanning 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 11, MS Defender SmartScreen can provide this functionality. **CE Requirement**: If you use anti-malware software to protect your device it must be configured to: • prevent connections to malicious websites over the internet.	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, Chromebooks, mobile phones and tablets restrict you from installing unsigned applications. Usually you have to "root" or "jailbreak" a device to allow unsigned applications. **CE Requirement**: Only approved applications, restricted by code signing, are allowed to execute on devices.	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. **CE Requirement:** • actively approve such applications before deploying them to devices • maintain a current list of approved applications, users must not be able to install any application that is unsigned or has an invalid signature	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