Cyber Essentials Scheme

Report date: 4/8/2023
Applicant: NetFM UK Ltd,
Validated by: David Herring, Founder

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

Congratulations, you have been successful in your assessment under the Cyber Essentials scheme. Your certificate number is **54524182-2912-4108-8121-ea10af67dda6** and can be found here:

https://registry.blockmarktech.com/certificates/54524182-2912-4108-8121-ea10af67dda6/

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.	NetFM UK Limited	Compliant Assessor Notes: According to the Companies House, the registration name is: NetFM UK Limited. Please correct the answer. *** Resubmission Notes *** The answer was corrected.
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.	08165293	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: Withycombe Address Line 2: Church Road East Town/City: Crowthorne County: Berkshire Postcode: RG45 7ND Country: United Kingdom	Assessor Notes: According to the Companies House, the registered address is: Withycombe, Church Road East, Crowthorne, Berkshire, England, RG45 7ND. Please correct the answer. *** Resubmission Notes *** The answer was corrected.
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".*	New Application	Compliant
A1.8 Reason for Certification **What are the two main reasons for applying for certification?** *Please let us know the two main reasons why you are applying for certification. If there are multiple reasons, please select the two that are most important to you. This helps us to understand how people are using our certifications.*	Required for Government Contract Custom Fields: Secondary Reason: To Give Confidence to Our Customers	Compliant
A1.8.2 Government Contracting Organisation **Who is the government contracting organisation and the contract number?**	Nottinghamshire County Council Tender Ref: DN665028	Compliant

Please provide the contract number and the contracting organisation.		
A1.9 CE Requirements Document **Have you read the 'Cyber Essentials Requirements for IT Infrastructure' document?** *Document is available on the NCSC Cyber Essentials website and should be read before completing this question set. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*	Yes	Compliant
A1.10 Cyber Breach **Can IASME and their expert partners contact you if you experience a cyber breach?** *We would like feedback on how well the controls are protecting organisations. If you agree to this then please email security@iasme.co.uk if you do experience a cyber breach. IASME and expert partners will then contact you to find out a little more but all information will be kept confidential.*	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 apply for insurance.** *Your whole organisation includes all divisions, people and devices which access your organisation's data and services.*	Yes	Compliant
A2.3 Geographical Location **Please describe the geographical locations of your business which are in the scope of this assessment.** *You should provide either a broad description (i.e. All UK offices) or simply list the locations in scope (i.e. Manchester and Glasgow retail stores).*	No central office location - all homeworks	Compliant Assessor Notes: Please be consistent with all the answers and include all the geographical locations that fall within the scope of the assessment. For example, the answer of A2.5 refers to a server in France. *** Resubmission Notes *** It appears from the updated answer that the locations that fall within the scope of the assessment include an office located in the UK, a tenancy of a datacentre located in the UK, and another tenancy of a datacentre located in France. *** Second Resubmission Notes ***

		The location of each homeworker is provided in the answer of A2.7.
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.*	4 macbook pro + macOS 13: Ventura (Rome) 1 IBM thinkpad + Ubuntu 22.04 3 HP Notebooks + Windows 10 Pro + 22H2 + 19045.3208 3 desktops: 1 NUC + Ubuntu 22.04 2 Mac desktops i24 + macOS 13: Ventura (Rome)	Compliant Assessor Notes: 1. Please provide the answer with the requested details. If unsure, please refer to the examples. 2. Please remove the details of the mobile phones from this answer. *** Resubmission Notes *** Please provide the requested details: - Versions of macOS operating systems. - Edition and version of Windows 10. *** Second Resubmission Notes *** Please provide the edition and version of Windows 10. *** Third Resubmission Notes *** Please provide the edition of Windows 10. *** Fourth Resubmission Notes *** The answer was updated.
A2.4.1 Thin Client Devices **Please list the quantity of thin clients within scope of this assessment. Please include make and operating systems.** *Please provide a summary of all the thin clients in scope that are connecting to organisational data or services (Definitions of which are in the 'CE Requirements for Infrastructure document' linked in question A1.9).* *Thin clients are commonly used to connect to a Virtual Desktop Solution.* ***Thin clients are a type of very simple computer holding only a base operating system which are often used to connect to virtual desktops. Thin clients can connect to the internet, and it is possible to modify some thin clients to operate more like PCs, and this can create security complications. Cyber Essentials requires thin clients be supported and receiving security updates.***	None	Compliant

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*	5 x Ubuntu + 22.04 LTS 4 x Ubuntu + 22.04 LTS + VM's + AHV hypervisor + 20201105.2096 No physical servers outside of OVH datacentre full within the scope of this assessment	Compliant Assessor Notes: Please provide a structured answer. For example: quantity x server operating system brand + edition + version. If servers are hosted by a hypervisor, please provide its brand and version. If the hypervisor is deployed on a physical server, please provide its brand and model. There is no need to provide the specifications of the server or any details regarding containers or container orchestrators. *** Resubmission Notes *** 1. Please provide the version of the Nutanix Acropolis Hypervisor (AHV). 2. Please confirm that no physical servers fall within the scope of the assessment. *** Second Resubmission Notes *** 1. Please provide the version of the Nutanix Acropolis Hypervisor (AHV). 2. Please confirm that no physical servers fall within the scope of the assessment. 3. Please refer to the last Assessor Notes of A2.7. *** Third Resubmission Notes *** The answer was updated.
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.*	6 x Apple iPhones with iOS 15.7.7 6 x Google Pixel 6 with Android 13	Compliant Assessor Notes: Please provide the answer with the requested details. That is: quantity x device + operating system + version (e.g., 2 x Apple iPhones with iOS 16.5.1 (c)). *** Resubmission Notes *** The answer was updated.

A2.7 Networks **Please provide a list of your networks that will be in the scope for this assessment.** *You should include details of each network used in your organisation including its name, location and its purpose (i.e. Main Network at Head Office for administrative use, Development Network at Malvern Office for testing software, home workers network - based in UK).* *You do not need to provide IP addresses or other technical information.* *For further guidance see the Home Working section in the 'CE Requirements for Infrastructure Document'.* https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf	Server network at OVH London - dedicated servers and dedicated edge network firewall Home workers network - based UK :- Crowthorne - Dave Camberley - Nici Chobham - Mark Ealing - Ben Cambridge - Finlay Bristol - Sam we do not provide routers or any access equipment - just the computer device (Mac book pro or windows ThinkPad laptop). The responsibility lies with the homeworker to apply a 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 Assessor Notes: Please provide the answer with the requested details. If unsure, please refer to the examples. *** Resubmission Notes *** 1. The updated answer does not assist in understanding the scope of the assessment. For example, there is a declared office location but there is no network. In addition, the network of the datacentre is also included but it is not clear what services this service provider offers. Is it a public cloud, private cloud, physical datacentre tenancy? Unless the scope of the assessment is clearly defined without ambiguities, this assessment cannot continue (i.e., answers will be marked with More Information Required scores). 2. Please consult the 'CE Requirements for Infrastructure Document' (https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf) and decide the locations, networks, network devices, server devices, hypervisors, and server operating systems that fall within the scope of the assessment. *** Second Resubmission Notes *** Please consult the service provider, it appears to be OVHcloud, and the 'CE Requirements for Infrastructure Document' (https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf) and decide the scope of this assessment. Introducing the term IaaS in this answer and then including a hypervisor in the answer of A2.5, leaves ambiguities and the conclusion is that the organisation is not aware of the services consumed by the service provider. *** Third Resubmission Notes *** The answer was updated.
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*	9 home workers	Compliant Assessor Notes: Please provide the number of homeworkers. *** Resubmission Notes *** The answer was updated.

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.*	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 Assessor Notes: 1. Please provide the answer with the requested details. It is unclear what network devices, physical or virtual, fall within the scope of this assessment, and where these devices are located. 2. Assuming that there is an office somewhere, there must be at least one router with embedded firewall in this office to manage the network traffic between the LAN of the office, and whatever other LANs (e.g., LANs of homeworkers, LAN of an IaaS tenancy, LAN of a datacentre tenancy, etc.) are connected via a WAN. Please provide the brand and model of each device. *** Resubmission Notes *** 1. If the organisation does not use an office for the members of staff, then it has to be removed from the answer of A2.3 that requires the geographical locations. 2. The updated answer claims that 'OVH based servers have built sophisticated edge firewalls'. This sentence is confusing because edge firewalls are boundary firewalls and not firewalls that are part of servers. If the organisation uses boundary firewalls, physical or virtual, then please list their brand and model. 3. Please consult the 'CE Requirements for Infrastructure Document' (https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf) and decide the locations, networks, network devices, server devices, hypervisors, and server operating systems that fall within the scope of the assessment. *** Second Resubmission Notes *** The updated answer is not aligned with the question, which in turn, requires a list of the network devices, physical or virtual, that fall within the scope of this assessment. In the answer of A2.7, there is a reference to an edge firewall. Please clarify what type of firewall it is (e.g., physical, virtual, service). In addition, since there is no office and members of staff work from home, please include in the answer that software firewalls act as the boundary for homeworkers. *** Third Resubmission Notes *** 1. The organisation has confirmed that the edge firewall is a cloud service and not a virtual appliance. 2. The updated answer claims that this firewall acts as the boundary for all homeworkers when accessing the servers of the OVHcloud. This claim is wrong because this edge firewall cloud service acts as the network boundary security control of the servers, while the boundary security control of the homeworkers is provided by their software firewalls.

A2.9 Cloud Services Please list all of your cloud services that are in use by your organisation and provided by a third party. **Please note cloud services cannot be excluded from the scope of CE.** *You need to include details of all of your cloud services. This includes all types of services - IaaS, PaaS and SaaS. Definitions of the different types of Cloud Services are provided in the 'CE Requirements for Infrastructure Document'.* https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf	OVH Dedicated server center servers GitLab Sourece code contril Security scanning on source code Automated deployments and testing prior Google Full Workplace suite Gmail + Gdocs + 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 Total Gross Revenue **What is your total gross revenue? Please**	700K	Compliant

provide figure to the nearest £100K. You only need to answer this question if you are taking the insurance. *The answer to this question will be passed to the insurance broker in association with the cyber insurance you will receive at certification. Please be as accurate as possible - figure should be to the nearest £100K.*		
A3.4 Insurance Email Contact **What is the organisation email contact for the insurance documents? You only need to answer this question if you are taking the insurance.** *The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification and they will use this to contact you with your insurance documents and renewal information.*	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.*	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 **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.	Windows defender on Windows PCs for homeworkers Mac firewall service on Macs UFW - Uncomplicated firewall on Linux based devices	Compliant Assessor Notes: Please provide the answer with the requested details. *** Resubmission Notes *** The answer was updated.
A4.2 Firewall Default Password **When you first receive an internet router or hardware firewall device, it may have had a default password on it. Have you changed all the default passwords on your boundary firewall devices?** *The default password must be changed*	Yes Custom Fields: Applicant Notes: This is done as part of our standard server setup process.	Compliant

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.*	The OVH based servers have an edge firewall that can be set from the dedicated OVH secure web-portal: 1. Login to OVH web portal using known email / password combination + confirm 2FA auth on mobile phone. 2. Go to account profile, and set a new password We educate homeworkers to set their own OS firewall on their chosen device to only allow connections on standard ports and disable all incoming connections. The OS password change process for is different for each OS type: Ubuntu laptop 1. Login to device using standard user account 2. Become an super user (administrator) using sudo su - 3. Change the user account password Windows laptop 1. Acess Start-> Settings -> Accounts -> Sign in options 2. Select password change 3. Enter original three word + date password 4. Enter new three word + date password 5. Repeat to confirm typed correctly 6. Confirm password change MaxOS Password Change 1. Apple menu > System Settings, then click Users & Groups in the sidebar. 2. Clickthe Info button next to your username on the right 3. Click Change Password. 4. Enter your current password in the Old Password field. 5. Enter your new password in the New Password field, then enter it again in the Verify field. 6. For help choosing a secure password, click the Key button next to the New Password field. (Follow NetFM guideance - xreate a three word + date password. 7. Optionally enter a hint to help you	Compliant Assessor Notes: Please describe the process, as a sequence of steps, for changing the password of the boundary firewalls (physical or virtual). If a software firewall is being relied on as the network boundary, please describe how its local admin password is changed. *** Resubmission Notes *** 1. Cyber Essential Assessments do not offer the option for the organisation to select what to include in the answers of the questions. If the organisation would like to reduce the scope of the assessment to focus on the services offered, then the scope of the assessment needs to be redefined. Otherwise, please expand the answer to include all the software firewalls. *** Second Resubmission Notes *** The organisation is accountable for the security controls that fall within the scope of this assessment, including the software firewalls of people who work from home because their firewalls become the boundary firewalls. Please expand the answer to describe how the local admin passwords of these firewalls are changed. Please bear in mind that homeworkers use three different operating systems. *** Third Resubmission Notes *** According to the updated answers provided by the organisation, there are individual LANs used by homeworkers. The firewall security controls of each of these LANs is represented by the software firewall of each End User Device (EUD) used by the homeworkers. This is because Cyber Essentials exclude ISP routers/firewalls from the scope of the assessment. Each of these LANs connects to the network provided by OVHcloud (i.e., another virtual LAN) via the Internet. The edge firewall service represents the firewall security control that protects this virtual LAN, where servers are part of, from the untrusted network, which is the Internet. Please expand the answer to describe how the local admin passwords of these software firewalls are changed. Please bear in mind that homeworkers use three different operating systems.

	remember the password. 8. Click Change Password.	*** Fourth Resubmission Notes *** Please include the remaining operating systems in the answer (i.e., macOS and Windows). *** Fifth Resubmission Notes *** The answer was updated.
A4.3 Firewall Password Configuration Is your new firewall password configured to meet the 'Password-based authentication' requirements? Please select the option being used. A. Multi-factor authentication, with a minimum password length of 8 characters and no maximum length B. Automatic blocking of common passwords, with a minimum password length of 8 characters and no maximum length C. A minimum password length of 12 characters and no maximum length D. None of the above, please describe *Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the new section about password-based authentication in the 'Cyber Essentials Requirements for IT Infrastructure' document.* https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf	0: A. Multi-factor authentication with a minimum password length of 8 characters and no maximum length 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.*	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 Services **Do you have any services enabled that can be accessed externally through your internet router, hardware firewall or software firewall?** *At times your firewall may be configured to allow a system on the inside to become accessible from the internet (for example: a VPN server, a mail server, an FTP server or a service that is accessed by your customers). This is sometimes referred to as "opening a port". You need to show a business case for doing this because it can present security risks. If you have not enabled any services, answer "No". By default, most firewalls block all services.*	Yes Custom Fields: Applicant Notes: 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.	Compliant
A4.5.1 Firewall Documented Business Case **Do you have a documented business case for all of these services?** *The business case should be documented and recorded. A business case must be signed off at board level and associated risks reviewed regularly.*	Yes Custom Fields: Applicant Notes: Documented on the NetFM company wiki	Compliant
A4.6 Firewall Service Process **If you do have services enabled on your firewall, do you have a process to ensure they are disabled in a timely manner when they are no longer required? A description of the process is required.** *If you no longer need a service to be enabled on your firewall, you must remove it to reduce the risk of compromise. You should have a process that you follow to do this (i.e. when are services reviewed, who decides to remove the services, who checks that it has been done?).*	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 fireall 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 Assessor Notes: Please describe the process, as a sequence of steps, that covers how the removal of a business service (e.g., due to disposal or change) triggers the realignment of security controls, including the reconfiguration of the boundary firewall, in a timely manner. *** Resubmission Notes *** Please describe the process, as a sequence of steps, that covers how the removal of a business service (e.g., due to disposal or change) triggers the realignment of security controls, including the reconfiguration of the boundary firewall, in a timely manner. *** Second Resubmission Notes *** It is irrelevant if no additional services have been added to the firewall. Since this firewall has services enabled, please describe the process, as a sequence of steps, that covers how the removal of a business service (e.g., due to disposal or change) triggers the realignment of security controls, including the reconfiguration of the boundary firewall, in a timely manner. *** Third Resubmission Notes *** Changing the rules of firewalls without control may lead to two different scenarios. The first includes denial of

		service conditions where the rules are changed in a way to block legitimate requests, whereas the second includes the introduction of backdoors that might be exploited by threat actors. Both scenarios are subject to uncontrolled changes where the organisation is unable to distinguish authorised from unauthorised changes. It is therefore strongly recommended to include the business service changes under change management, where the alteration or decommissioning of a business service is assessed from different perspectives, including security. If changes are agreed, they should be authorised to cover the affected systems, including firewalls.
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: Only port 443 - SSL web access is generally available mon production servers. This is checked regularly inhouse using nmap, and periodically by client request using a formal pen test.	Compliant
A4.8 Firewall Remote Configuration **Are your boundary firewalls configured to allow access to their configuration settings over the internet?** *Sometimes organisations configure their firewall to allow other people (such as an IT support company) to change the settings via the internet.* *If you have not set up your firewalls to be accessible to people outside your organisations or your device configuration settings are only accessible via a VPN connection, then answer "no" to this question.*	No Custom Fields: Applicant Notes: Only access is from with OVH datacentre by dedicated staff	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*	Yes	Compliant Assessor Notes: Applicant Notes are optional. Please ensure these are relevant to the question. If they are not, they don't add any value but ambiguities. By adding a note that UFW is deployed on all servers, and no comment is made on End User Devices (EUDs), it implies that these devices don't have any software deployed or enabled. Please either expand the Applicant Notes to add what

by going to Settings and searching for "Windows firewall". On Linux try "ufw status".		has been deployed on EUDs or remove the notes completely as they don't help. *** Resubmission Notes *** The Applicant Notes were removed.
A5.1 Removed Unused Software **Where you are able to do so, have you removed or disabled all the software and services that you do not use on your laptops, desktop computers, thin clients, servers, tablets, mobile phones and cloud services? Describe how you achieved this.** *You must remove or disable all applications, system utilities and network services that are not needed in day-to-day use. You need to check your cloud services and disable any services that are not required for day-to-day use.* *To view your installed applications:* *1. Windows by right clicking on Start ? Apps and Features* *2. macOS open Finder -> Applications* *3. Linux open your software package manager (apt, rpm, yum).*	We regularly run Linux apt autoremove 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. Homeworkers based machines are under the direct control of the homeworker. They are regularly updated by individual developers who are skilled in the software removeal 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 Assessor Notes: Please include in the answer all the devices and services that fall within the scope of the assessment. That is, laptops, desktop computers, servers, mobile phones, and cloud services. *** Resubmission Notes *** The answer was updated.
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: Personal devices are under the direct control of that homeworker. All employees are provided a central google workplace login for access to company email and documnets and git-lab access for source code control. Login on homeworker devices is under the direct control of individual homeworkers.	Compliant Assessor Notes: Applicant Notes are optional. Please ensure these are relevant to the question. If they are not, they don't add any value but ambiguities. The answer must cover laptops, desktop computers, servers, mobile devices, and cloud services. It appears from the Applicant Notes that either the question has not been understood or the organisation cares about the servers only. Please provide the required clarification. *** Resubmission Notes *** The Applicant Notes were updated.
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*	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

common or predictable words such as "password" or "admin" or include predictable number sequences such as "12345".		
A5.4 Internally Hosted External Services **Do you run external services that provides access to data (that shouldn't be made public) to users across the internet?** *Your business might run software that allows staff or customers to access information across the internet to an external service hosted on the internal network, cloud data centre or IaaS cloud service. This could be a VPN server, a mail server, or an internally hosted internet application(SaaS or PaaS) that you provide to your customers as a product. In all cases, these applications provide information that is confidential to your business and your customers and that you would not want to be publicly accessible.*	Yes Custom Fields: Applicant Notes: Visitor Express uses private services that are run on OVH servers to provide internal support documentation. Visitor Express has dedicated private repos hosted on GitLab for each client customer. These allow clients to shown the live ticket updates that pertain only to them.	Compliant
A5.5 External Service Password Configuration **If yes to question A5.4, which option of password-based authentication do you use?** **A. Multi-factor authentication, with a minimum password length of 8 characters and no maximum length** **B. Automatic blocking of common passwords, with a minimum password length of 8 characters and no maximum length** **C. A minimum password length of 12 characters and no maximum length** **D. None of the above, please describe** *Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the section about 'Password-based authentication' in the 'Cyber Essentials Requirements for IT Infrastructure' document.* https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf	0: A. Multi-factor authentication with a minimum password length of 8 characters and no maximum length Custom Fields: Applicant Notes: Use bitwarden to maintain very strong passwords across all services.	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.**	We use bitarden 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:	Compliant Assessor Notes: Please describe the process, as a sequence of steps, for changing passwords when the organisation believes 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.	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	*** Resubmission Notes *** When it is believed that a password of an external service has been compromised, this information should come from somewhere, for example a user or any detection security control that is in place to detect suspicious activities. In such scenarios, it is recommended to raise a security incident and follow the required steps to contain the threats, eradicate them, and then recover the affected systems to their original states. The change of password belongs to the last step. Changing passwords straightaway cannot address scenarios where threats actors have already managed to escalate privileges and setup backdoors.
A5.7 External Service Brute Force **When not using multi-factor authentication, which option are you using to protect your external service from brute force attacks?** **A. Throttling the rate of attempts** **B. Locking accounts after 10 unsuccessful attempts** **C. None of the above, please describe** *The external service that you provide must be set to slow down or stop attempts to log in if the wrong username and password have been tried a number of times. This reduces the opportunity for cyber criminals to keep trying different passwords (brute-forcing) in the hope of gaining access.*	A. Throttling the rate of attempts	Compliant Assessor Notes: Applicant Notes are optional. Please ensure these are relevant to the question. If they are not, they don't add any value but ambiguities. It is unclear what the purpose of the Applicant Notes is. Throttling the rate of attempts is a security control that is used to protect passwords against brute-force attacks. Sometimes adversaries may use security controls to cause Denial of Service (DOS) conditions. But to use throttling the rate of attempts to cause a DOS attack simply raises the question, why not attack the server(s) that provide the services instead? In addition, why DDOS is referred? Please clarify the notes or just remove them. *** Resubmission Notes *** The Applicant Notes were removed.
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: Only one developer uses a windows device, and these are disabled on that device. Most developers use either Linux or Mac based 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?**	Yes Custom Fields: Applicant Notes: We use finger print access to development devices.	Compliant

Device locking mechanisms such as biometric, password or PIN, need to be enabled to prevent unauthorised access to devices accessing organisational data or services.		
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.	We do not control individual homeworker devices. Training encourages them to set a 2 minute inactivity lock screen with finger print reactivation. These are used solely to unlock personal devices and do not provide access to company servers or company infrastructure.	Compliant Assessor Notes: Please provide the answer with the requested details. If unsure, 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). *** Resubmission Notes *** Please confirm if these credentials are used solely to unlock devices and do not provide access to organisational data and services without further authentication. *** Second Resubmission Notes *** The updated answer is not aligned with the question. Please avoid removing previous answers because they provide continuity. Here is the previous answer provided by the organisation: Finger print + pin code The assessment requires the organisation to confirm if these credentials are used solely to unlock devices and do not provide access to organisational data and services without further authentication. *** Third Resubmission Notes *** The answer was updated.
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*	Yes	Compliant Assessor Notes: Applicant Notes are optional. Please ensure these are relevant to the question. If they are not, they don't add any value but ambiguities. It appears from the Applicant Notes that the question has not been understood. Please provide the required clarification as the question is not related to firewalls. *** Resubmission Notes *** The Applicant Notes were removed.

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.		
A6.2 Supported Software **Is all the software on your devices supported by a supplier that produces regular fixes for any security problems?** *All software used by your organisation must be supported by a supplier who provides regular security updates. Unsupported software must be removed from your devices. This includes frameworks and plugins such as Java, Adobe Reader and .NET.*	Yes Custom Fields: Applicant Notes: Ubuntu 22.04.2 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 reuired a reboot. A message is posted in the clients dedicated WhatsApp support group prior to any updates that require a server reboot. Postgres 15.3 - 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 1.5 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 102, Safari Version 15.*	Firefox 115.0 (64-bit) Safari v16.0 Chrome 115.0.5790.98	Compliant Assessor Notes: Google Chrome 114.0.5735.106 was released on 05/06/2023. Since then, a few updates that contain security fixes have been released. The omission to apply these updates within the 14-day window causes a Major Non-Compliance score in A6.5. Please apply the missing patches and update this answer. *** Resubmission Notes *** Google Chrome 114.0.5735.106 was released on 05/06/2023. Since then, a few updates that contain security fixes have been released. The omission to apply these updates within the 14-day window causes a Major Non-Compliance score in A6.5. Please apply the missing patches and update this answer. *** Second Resubmission Notes *** Google Chrome 114.0.5735.106 was released on 05/06/2023. Since then, a few updates that contain security fixes have been released. The omission to

		apply these updates within the 14-day window causes a Major Non-Compliance score in A6.5. Please apply the missing patches and update this answer. *** Third Resubmission Notes *** It appears that Google Chrome was upgraded to version 115.0.5790.98.
A6.2.2 Malware Protection **Please list your Malware Protection software. The version is required.** *Please list all malware protection and versions you use so that the Assessor can understand your setup and verify that they are in support.* *For example: Sophos Endpoint Protection V10, Windows Defender, Bitdefender Internet Security 2020.*	ClamAV 1.1.0 Windows Defender KB2267602 Mac standard firewall - macOS 13 Ventura	Compliant Assessor Notes: 1. Pleaser provide the version of ClamAV. 2. The scope of the assessment also includes macOS and Windows operating systems. Please include their antimalware software and version in this answer. *** Resubmission Notes *** The answer was updated.
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.*	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.*	Google Workspace	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*	Yes Custom Fields: Applicant Notes: Licenses: PostgreSQL License, a liberal Open Source license, similar to the BSD or MIT licenses. PostgreSQL Database Management	Compliant

systems, firmware and applications, if annual licensing is not purchased, they will not be receiving regular security updates.	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	
A6.4 Security Updates - Operating System **Are all high-risk or critical security updates for operating systems and router and firewall firmware installed within 14 days of release?** *You must install all high and critical security updates within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question. You are not required to install feature updates or optional updates in order to meet this requirement.* *This requirement includes the firmware on your firewalls and routers.*	Yes Custom Fields: Applicant Notes: 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.*	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 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.*	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 One a week we manually login to all servers and check the latest updates have been applied. Sometime 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	Compliant Assessor Notes: This question applies to all operating systems and firmware of all devices included in the scope of the assessment. Please describe how the organisation ensures that all high-risk or critical security updates of all operating systems and firmware are applied within 14 days of release when auto updates are not supported, are not enabled, or they fail. *** Resubmission Notes *** Please describe how the organisation ensures that homeworkers apply all high-risk or critical security updates of all operating systems and firmware within 14 days of release when auto updates are not supported, are not enabled, or they fail. *** Second Resubmission Notes *** The answer was updated.

	homeworker devices.	
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: Chrome updated to latest	Compliant Assessor Notes: 1. According to the answer of A6.2.1, Google Chrome 114.0.5735.106 is the latest deployed version, which was released on 05/06/2023. Since then, a few updates that contain security fixes have been released. Please apply the missing patches and update the answer of A6.2.1. 2. The Applicant Notes are not aligned with the question. Please, align them with the question or remove them. *** Resubmission Notes *** 1. According to the answer of A6.2.1, Google Chrome 114.0.5735.106 is the latest deployed version, which was released on 05/06/2023. Since then, a few updates that contain security fixes have been released. Please apply the missing patches and update the answer of A6.2.1. 2. The Applicant Notes were removed and the answer was changed to 'No'. *** Second Resubmission Notes *** According to the answer of A6.2.1, Google Chrome 114.0.5735.106 is the latest deployed version, which was released on 05/06/2023. Since then, a few updates that contain security fixes have been released. Please apply the missing patches and update the answer of A6.2.1. *** Third Resubmission Notes *** According to the answer of A6.2.1, Google Chrome was upgraded to version 115.0.5790.98.
A6.5.1 Auto-Updates - Applications **Are all updates applied on your applications by enabling auto updates?** *Most devices have the option to enable auto updates. Auto updates should be enabled where possible.*	Yes	Compliant Assessor Notes: The Applicant Notes are not aligned with the question. Please align them with the question or remove them. *** Resubmission Notes *** The Applicant Notes are not aligned with the question. Please align them with the question or remove them. *** Second Resubmission Notes *** The Applicant Notes were removed.
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?**	Two types of applicatoj 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	Compliant Assessor Notes: This question applies to all applications of all devices included in the scope of the assessment. Please describe how the organisation ensures that all high-risk or

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.*	(continuous integration / continuous delivery) scripts that run immediately on any sourvce 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 enure the latest updates have been applied. Other OS supplied browsers are maintained up to date by OS updates. If a hoem worker elects to use Firefox, then the same update manual checking method is app,ied to this, Home workers mainly use vscode for software development, thi has an uatomatic check for updates on start up, 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 updates these as part of the build process. This only runs on the production servers, but ensure the latest fully supported packages are bundled with each build.	critical security updates of all applications are applied within 14 days of release when auto updates are not supported, are not enabled, or they fail. *** Resubmission Notes *** This question focuses on applications and not operating systems. Please correct the answer. *** Second Resubmission Notes *** Please avoid removing previous answers because they provide continuity. Here is the previous answer: We login to each device server or homeworker device weekly and manually run any OS updates. The updated answer contradicts the previous one. Please bear in mind that the answers of the assessment must reflect the current state and practices of the organisation. That is, please avoid providing random answers for the purpose of passing the assessment. The devices used by homeworkers fall within the scope of the assessment. Please describe how the organisation ensures that all high-risk or critical security updates of all applications are applied within 14 days of release when auto updates are not supported, are not enabled, or they fail. *** Third Resubmission Notes *** This question focuses on software applications and not operating systems. Please correct the answer. *** Fourth Resubmission Notes *** The answer was updated.
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.*	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.*	#1 Google workplace 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 include checking an identification document (passport). To create the account:- 1. Operations directory logs into Google workplace using 2FA 2. Creates an email aliase 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 se;lect Linux / Windows 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 22.04 LTS desktop version 2. Setup username as firstname 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	Compliant Assessor Notes: This question applies to all user accounts of the devices and services that fall within the scope of the assessment. Please describe the process, as a sequence of steps, which is followed by the organisation to provision user accounts. *** Resubmission Notes *** This question applies to all user accounts of the devices and services that fall within the scope of the assessment. Please describe the process, as a sequence of steps, which is followed by the organisation to provision user accounts. *** Second Resubmission Notes *** This question requires the description of the process. Please describe the process, as a sequence of steps, which is followed by the organisation to provision user accounts. *** Third Resubmission Notes *** The updated answer keeps focusing on Google Workplace user accounts. This question applies to all user accounts of the devices and services that fall within the scope of the assessment (e.g., user accounts for Windows EUDs, macOS EUDs, Linux EUDs, Linux servers, OVHcloud service, GitLab service, etc.). Please describe the process, as a sequence of steps, which is followed by the organisation to provision user accounts. *** Fourth Resubmission Notes *** This question applies to all user accounts of the devices and services that fall within the scope of the assessment (e.g., user accounts for Windows EUDs, macOS EUDs, Linux EUDs, Linux servers, OVHcloud service, GitLab service, etc.). Please describe the process, as a

	designated account created for them 5. A separate administrator account is created by operations director - that homeworker does not have access to. #3 Windows account - home device 1. Install Windows 10 Pro + 22H2 + 19045.3208 2. Setup an account with the firstname 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. #4 Mac account - home device 1. Install macOS 13: Ventura (Rome) 2. Setup an account with the firstname 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 workd + date password. They are not allowed to creat more accounts on their home device They are not allowed to use their home device other than for company business usingnthe 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 hsosted servers using ssh for adnministrations. 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. Creat account with same username as	sequence of steps, which is followed by the organisation to provision user accounts. *** Fifth Resubmission Notes *** The answer was updated.

	the homeworker uses on home device 5. Create a strong three work + date password usiq for that end user to access OVH 6. Select 2FA - enter home workers mobile number 7. Click create account	
A7.2 Unique Accounts **Are all your user and administrative accounts accessed by entering a unique username and password?** *You must ensure that no devices can be accessed without entering a username and password.* **Accounts must not be shared.**	Yes	Compliant
A7.3 Leavers Accounts **How do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation?** *When an individual leaves your organisation you need to stop them accessing any of your systems.*	We manually audit the active accounts - only 8 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 aliase 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 Assessor Notes: Please describe the process, as a sequence of steps, that is followed by the organisation to ensure that any accounts for members of staff who are no longer with the organisation are disabled or deleted immediately to prevent unauthorised access. *** Resubmission Notes *** This question applies to all user accounts of the devices and services that fall within the scope of the assessment. Please describe the process, as a sequence of steps, that is followed by the organisation to ensure that any accounts for members of staff who are no longer with the organisation are disabled or deleted immediately to prevent unauthorised access. *** Second Resubmission Notes *** Please describe the process, as a sequence of steps, that is followed by the organisation to ensure that any accounts for members of staff who are no longer with the organisation are disabled or deleted immediately to prevent unauthorised access. *** Third Resubmission Notes *** The updated answer keeps focusing on Google Workplace user accounts. This question applies to all user accounts of the devices and services that fall within the scope of the assessment (e.g., user accounts for Windows EUDs, macOS EUDs, Linux EUDs, Linux servers, OVHcloud service, GitLab service, etc.). Please describe the process, as a sequence of steps, that is followed by the organisation to ensure that any accounts

		for members of staff who are no longer with the organisation are disabled or deleted immediately to prevent unauthorised access. *** Fourth Resubmission Notes *** This question applies to all user accounts of the devices and services that fall within the scope of the assessment (e.g., user accounts for Windows EUDs, macOS EUDs, Linux EUDs, Linux servers, OVHcloud service, GitLab service, etc.). Please describe the process, as a sequence of steps, that is followed by the organisation to ensure that any accounts for members of staff who are no longer with the organisation are disabled or deleted immediately to prevent unauthorised access. *** Fifth Resubmission Notes *** The answer was updated.
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.*	# Google workplace accounts Manually audit all the 8 accounts in Google workplace - only 8 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. Clicks the email aliase 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 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. Windows 1. Login as the company home device	Compliant Assessor Notes: Please describe the process, as a sequence of steps, which is followed by the organisation to ensure that members of staff only have the privileges that they need to do their current job. That is, how does the organisation ensure that the permissions assigned to the system roles or groups are not under-provisioned to prevent denial of service conditions and they are not overprovisioned to prevent misuse? Please also include the scenario where a user changes business role. *** Resubmission Notes *** This question applies to all user accounts of the devices and services that fall within the scope of the assessment. Please describe the process, as a sequence of steps, which is followed by the organisation to ensure that members of staff only have the privileges that they need to do their current job. That is, how does the organisation ensure that the permissions assigned to the system roles or groups are not under-provisioned to prevent denial of service conditions and they are not overprovisioned to prevent misuse? Please also include the scenario where a user changes business role. *** Second Resubmission Notes *** Please describe the process, as a sequence of steps, which is followed by the organisation to ensure that members of staff only have the privileges that they need to do their current job. That is, how does the organisation ensure that the permissions assigned to the system roles or groups are not under-provisioned to prevent denial of service conditions and they are not overprovisioned to prevent misuse? Please also include the scenario

	administrator account 2. Select Start > Settings > Accounts . 3. Under Family & other users, select the account owner name (you should see "Local account" below the name), then select Change account type. ... 4. Under Account type, select Administrator, and then select OK. 5. Ask home worker to Sign in with the their new administrator account to check access. # 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 root password, 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 accoiunts created for them on the OVH web portal.	where a user changes business role. *** Third Resubmission Notes *** The updated answer keeps focusing on Google Workplace user accounts. This question applies to all user accounts of the devices and services that fall within the scope of the assessment (e.g., user accounts for Windows EUDs, macOS EUDs, Linux EUDs, Linux servers, OVHcloud service, GitLab service, etc.). Please describe the process, as a sequence of steps, which is followed by the organisation to ensure that members of staff only have the privileges that they need to do their current job. That is, how does the organisation ensure that the permissions assigned to the system roles or groups are not under-provisioned to prevent denial of service conditions and they are not overprovisioned to prevent misuse? Please also include the scenario where a user changes business role. *** Fourth Resubmission Notes *** This question applies to all user accounts of the devices and services that fall within the scope of the assessment (e.g., user accounts for Windows EUDs, macOS EUDs, Linux EUDs, Linux servers, OVHcloud service, GitLab service, etc.). Please describe the process, as a sequence of steps, which is followed by the organisation to ensure that members of staff only have the privileges that they need to do their current job. That is, how does the organisation ensure that the permissions assigned to the system roles or groups are not under-provisioned to prevent denial of service conditions and they are not overprovisioned to prevent misuse? Please also include the scenario where a user changes business role. *** Fifth Resubmission Notes *** Please ensure that user accounts and privileges are always provisioned according to the business roles undertaken by users.
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.*	User access levels changes for home devices , Google workplace, and OVH servers has to 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.	Compliant Assessor Notes: Please describe the process, as a sequence of steps, for giving someone access to systems at an administrator level. Please include the name of the business role that approves the request. *** Resubmission Notes *** This question applies to all admin accounts of the devices and services that fall within the scope of the assessment. Please describe the process, as a sequence of steps, for giving someone access to systems at an administrator level. Please include the name of the business role that approves the request. *** Second Resubmission Notes ***

	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 diretcor, who can login using the company administrator account for home devices and make the change for the homeworkers account on that device.	This question requires the description of the process and must cover all systems that fall within the scope of the assessment, including the devices used by homeworkers. Please describe the process, as a sequence of steps, for giving someone access to systems at an administrator level. *** Third Resubmission Notes *** 1. This question requires the description of the process, as a sequence of steps, for giving someone access to systems at an administrator level. Generic answers indicate that the organisation doesn't have a process. It is therefore advised to create a process and describe it in this answer as a sequence of steps. Please also ensure this process covers all system admin accounts. 2. The claim that the access to any home based computer does not give access to the company services and servers stands true until this computer is compromised by threat actors because its user has not used the system admin account properly. 3. If the administrator level access to home based devices is under the direct control of homeworkers, it implies that the organisation cannot manage the access to these administrator accounts. Therefore, claiming in the answers of A7.8 and A7.9 that the organisation can track and review all admin access is an exercise that currently cannot be achieved. Consequently, the answers of both questions will result in a Major Non-Compliance score. 4. Google Workplace is the former Google G Suite SaaS, which is a productivity suite of applications. Please confirm what application of this SaaS offering enables admin access to the tenancy of OVHcloud, its services, and its Linux servers at a system administration level. *** Fourth Resubmission Notes *** 1. This question requires the description of the process, as a sequence of steps, for giving someone access to systems at an administrator level. Generic answers indicate that the organisation doesn't have a process. It is therefore advised to create a process and describe it in this answer as a sequence of steps. It is recommended to include in the process who requests the administrative access, for what reason, what systems need to be accessed, for how long, and who approves the access. The approver needs to be a business role of the senior leadership team. Please also ensure this process covers all system admin accounts. 2. If the administrator level access to home based devices is under the direct control of homeworkers, it implies that the organisation cannot manage the access to these administrator accounts.

		Therefore, the administrative access that covers homeworkers should be included in the requested process of this question, and their request for access should be subject to approval. *** Fifth Resubmission Notes *** The answer was updated.
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.*	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 there 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 acconts to access the servers with 2FA. These onlly 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.	Compliant Assessor Notes: Please describe how the organisation ensures that administrator accounts are used only to carry out administrative tasks (e.g., installing software or making configuration changes) and system administrators do not misuse the computer accounts by remaining logged on to these accounts permanently. *** Resubmission Notes *** This question applies to all admin accounts of the devices and services that fall within the scope of the assessment. Please describe how the organisation ensures that administrator accounts are used only to carry out administrative tasks (e.g., installing software or making configuration changes) and system administrators do not misuse the computer accounts by remaining logged on to these accounts permanently. *** Second Resubmission Notes *** This question applies to all admin accounts of the devices and services that fall within the scope of the assessment, including the admin accounts used by homeworkers to maintain their own devices. Please describe how the organisation ensures that administrator accounts are used only to carry out administrative tasks (e.g., installing software or making configuration changes) and system administrators do not misuse the computer accounts by remaining logged on to these accounts permanently. *** Third Resubmission Notes *** The answer was updated.
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*	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	Compliant Assessor Notes: Please describe how the organisation prevents administrator accounts from being used to carry out daily tasks, like browsing the web, accessing email, or chatting? *** Resubmission Notes *** This question applies to all admin

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.*	have a basic user account on their device for acess and doing their day to day work, with a separate administrator account that can install packages and perform upgrades on their home based device.	accounts of the devices and services that fall within the scope of the assessment. Please describe how the organisation prevents administrator accounts from being used to carry out daily tasks, like browsing the web, accessing email, or chatting? *** Second Resubmission Notes *** This question applies to all admin accounts of the devices and services that fall within the scope of the assessment, including the admin accounts used by homeworkers to maintain their own devices. Please describe how the organisation prevents administrator accounts from being used to carry out daily tasks, like browsing the web, accessing email, or chatting? *** Third Resubmission Notes *** The answer was updated.
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: We track all access to the OVH portal for server administion. This is service is provided by OVH login logs, and is maintained by OVH. We track all server activity using standard system accounbting 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 Goog admin console, showing last login and login hostory. 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 Assessor Notes: *** Third Resubmission Notes *** According to the answer of A7.5, the administrator level access to home based devices is under the direct control of homeworkers, which implies that the organisation cannot manage the access to these administrator accounts. That is, currently the organisation cannot track all administration access. *** Fourth Resubmission Notes *** Due to the organisation structure, homeworkers will always be system administrators.
A7.9 Administrator Access Review **Do you review who should have administrative access on a regular basis?** *You must review the list of people with administrator access regularly. Depending on your business, this might be monthly, quarterly or annually. Any users who no longer need administrative access to carry out their role should have it removed.*	Yes Custom Fields: Applicant Notes: All home based workers (8 total) are trained and form par 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 8 local device administrator accounts form part of the company policy.	Compliant Assessor Notes: *** Third Resubmission Notes *** According to the answer of A7.5, the administrator level access to home based devices is under the direct control of homeworkers, which implies that the organisation cannot manage the access to these administrator accounts. That is, currently the organisation cannot review all administration access. *** Fourth Resubmission Notes *** Due to the organisation structure,

	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.	homeworkers will always be system administrators.
A7.10 Brute Force Attack Protection **Describe how you protect accounts from brute-force password guessing in your organisation?** *A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.* *Information on how to protect against brute-force password guessing can be found in the Password-based authentication section, under the User Access Control section in the 'Cyber Essentials Requirements for IT Infrastructure* *https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*	We have both 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 successful login.. Homebased workers are educated to setup auto lockout on their devices.	Compliant Assessor Notes: All passwords, guessable and unguessable, can be identified using brute-force attacks because adversaries try all possible combinations. If unsure about the question, please refer to the Password-based authentication section, under the User Access Control section in the Cyber Essentials Requirements for IT Infrastructure document (https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf). *** Resubmission Notes *** This question applies to all user accounts of the devices and services that fall within the scope of the assessment. Please include laptops, desktops, phones, and cloud services. *** Second Resubmission Notes *** By narrowing the answer, it explicitly excludes the user accounts that are not included in it. This question applies to all user accounts of the devices and services that fall within the scope of the assessment. Please include laptops, desktops, phones, and cloud services. *** Third Resubmission Notes *** The answer was updated.
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*	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 Assessor Notes: Please consult 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) and list the technical controls that are used to manage the quality of the passwords within the organisation. *** Resubmission Notes *** This question applies to all user accounts of the devices and services that fall within the scope of the assessment. Please list the technical controls that are used to manage the quality of the passwords within the organisation. *** Second Resubmission Notes *** Please consult 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) and list the technical controls that are used to manage the quality of the passwords within the organisation. *** Third Resubmission Notes *** The answer was updated.
A7.12 Password Creation Advice **Please explain how you encourage people to use unique and strong passwords.** *You need to support those that have access to your organisational data and services by informing them of how they should pick a strong and unique password.* *Further information can be found in the password-based authentication section, under the User Access Control section in the Cyber Essentials Requirements for IT Infrastructure* *document.* *https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*	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 Assessor Notes: Please refer to the Password-based authentication section, under the User Access Control section in the Cyber Essentials Requirements for IT Infrastructure document (https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf). *** Resubmission Notes *** Please refer to the Password-based authentication section in the Cyber Essentials Requirements for IT Infrastructure document and explain how the organisation encourages users to use unique and strong passwords. *** Second Resubmission Notes *** Bitwarden is a password management solution. It requires users to have their own master password and also to have configured rules for generating passwords. Please refer to the Password-based authentication section in the Cyber Essentials Requirements for IT Infrastructure document and explain how the organisation encourages users to use unique and strong passwords. *** Third Resubmission Notes *** The answer was updated.
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	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	0: A - Anti-Malware Software, 1: B - Limiting installation of applications by application allow listing from an approved app store	Compliant Assessor Notes: Please confirm how the organisation protects mobile devices against malware if Option B is not selected. *** Resubmission Notes *** According to previous answers, the organisation uses antimalware software systems. Please keep the initial Option A selected. *** Second Resubmission Notes *** The answer was updated.

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.		
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	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	Yes	Compliant

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.*		
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

IASME Consortium ®

SUTCLIFFE & CO.
INSURANCE BROKERS

Evidence of Insurance

Eligible Cyber Essentials Certificate Holders

Master Policy Number	**CY0538188**	
Master policy in the name of	**Holders of current Cyber Essentials Certificates**	
Cyber Essentials Certificate No.	54524182-2912-4108-8121-ea10af67dda6	
Insured Name	NetFM UK Limited	
Insured's Address	Withycombe,Church Road East,Crowthorne,Berkshire,RG45 7ND,United Kingdom	
Turnover	Up to £20,000,000	
Period of Insurance	From: 2023-08-04T21:39:00Z To: 2024-08-04T21:39:00Z Both days at 00:01 a.m.	
Insurer	AXA XL Insurance Company UK Limited	
Wording	Angel Cyber Essentials Liability insurance CYB 12/20 ANG.3 (https://www.sutcliffeinsurance.co.uk/all-insurance-products/cyber-insurance-data-protection-insurance/cyber-essentials-insurance/)	
Cyber Liability	Limit of Liability	£25,000 in the Aggregate (including defence costs and expenses)
	Excess	£1,000 per claim other than; £5,000 in respect of any loss from any claim emanating from activities in the USA or Canada
	BI Excess	6 hours
	Jurisdiction	UK & Crown Dependencies
	Geographical Limits	Worldwide
Retroactive Date	Inception date of the first cyber policy issued by Angel or Cyber Essentials Evidence of Insurance issued to the Insured. The retroactive date will be maintained at renewal providing there is no more than a 14 day gap from the end of the expiring Cyber Essentials certificate to the start of the renewing Cyber Essentials certificate.	

At first suspicion of an incident the organisation should immediately contact the **Accenture Response Hotline on 0800 085 9483.**

For Insurance questions please contact enquiries@sutcliffeinsurance.co.uk or call 01905 21681.