Cyber Essentials Scheme

Report date: 16/10/2025
Applicant: Collaboration Tools Ltd,

Validated by: Keith Harrison-Broninski, CEO

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

Congratulations, you have been successful in your assessment under the
Cyber Essentials (Willow) scheme. Your certificate number is **3fc88ab3-944d-4218-8915-40e349c1a54f** and can be found here:

https://registry.blockmarktech.com/certificates/3fc88ab3-944d-4218-8915-40e349c1a54f/

Your insurance number is 0038259873 and it can be found here:

https://registry.blockmarktech.com/certificates/e7d07f28-f3e1-46bd-8e86-03c424c055af/
The insurance certificate has been set to private, but can be viewed when
you register / log-in appropriately. We recommend keeping a hard copy or
separate copy of your insurance certificate / schedule in case you need
to make a claim and are unable to access your electronic copy. Both
your Cyber Essentials and Insurance certificates have been emailed to
you in separate messages as pdf attachments.

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

Applicant Answers

	Applicant Answers	Assessor Score
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
A1.1 Organisation Name? What is your organisation's name? The answer given in A1.1 is the name that will be displayed on your certificate and has a character limit of 150 including spaces. Where an organisation wishes to certify subsidiary companies on the same certificate, the organisation can certify as a group and can include the subsidiaries' name on the certificate as long as the board member signing off the certificate has authority over all certified organisations. For example: The Stationery Group, incorporating The Paper Mill and The Pen House It is also possible to list on a certificate where organisations are trading as other names. For example: The Paper Mill trading as The Pen House.	Collaboration Tools Ltd	Compliant

A1.2 Organisation Type What type of organisation are you? "LTD" – Limited Company (Ltd or PLC) "LLP" – Limited Liability Partnership (LLP) "CIC" – Community Interest Company (CIC) "COP" – Cooperative "MTL" – Other Registered Mutual (Community Benefit Society, Credit Union, Building Society, Friendly Society) "CHA" – Registered Charity "GOV" – Government Agency or Public Body "SOL" – Sole Trader "PRT" – Other Partnership "SOC" – Other Club/ Society "OTH" – Other Organisation	LTD - Limited Company (Ltd or PLC)	Compliant
A1.3 Organisation Number What is your organisation's registration number? Please enter the registered number only with **no spaces or other punctuation**. Letters (a-z) are allowed, but you need at least one digit (0-9). There is a 20 character limit for your answer. If you are applying for certification for more than one registered company, **please still enter only one organisation number**. If you have answered A1.2 with Government Agency, Sole Trader, Other Partnership, Other Club/Society or Other Organisation please enter "none". If you are registered in a country that does not issue a company number, please enter a unique identifier like a DUNS number.	06485797	Compliant
A1.4 Organisation Address What is your organisation's address? Please provide the legal registered address for your organisation.	UK Custom Fields: Address Line 1: 14 Horn Street Address Line 2: Nunney Town/City: Frome County: Somerset Postcode: BA11 4NP Country: United Kingdom	Compliant

A1.5 Organisation Occupation What is your main business? Please summarise the main occupation of your organisation.	IT	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://www.collaboration-tools.com	Compliant
A1.7 Renewal or First Time Application Is this application a renewal of an existing certification or is it the first time you have applied for certification? If you have previously achieved Cyber Essentials, please select "Renewal". If you have not previously achieved Cyber Essentials, please select "First Time Application".	Renewal	Compliant
A1.8 Reasons for Certification What are the two main reasons for applying for certification? Please let us know the two main reasons why you are applying for certification. If there are multiple reasons, please select the two that are most important to you. This helps us to understand how people are using our certifications.	Required for Government Contract Custom Fields: Secondary Reason: Required for Commercial Contract	Compliant
A1.8.2 Government Contract Organisation Who is the government contracting organisation and the contract number? Please provide the contract number and the contracting organisation.	600647, Innovate UK	Compliant

A1.9 CE Requirements Document Have you read the 'Cyber Essentials Requirements for IT Infrastructure' document? Document is available on the NCSC Cyber Essentials website and should be read before completing this question set. Cyber Essentials Requirements for IT Infrastructure v3.2	Yes	Compliant
A1.10 Cyber Breach Can IASME and their expert partners contact you if you experience a cyber breach? We would like feedback on how well the controls are protecting organisations. If you agree to this then please email security@iasme.co.uk if you do experience a cyber breach. IASME and expert partners will then contact you to find out a little more but all information will be kept confidential.	Yes	Compliant
A1.11 Contact Permission Can IASME contact you for research purposes? Both IASME and the UK government occasionally need to ask questions about the process and/or benefits of the Cyber Essentials scheme for research purposes. If you agree to this we will contact you via the email address you registered with, you are free to not respond if we do contact you.	Yes	Compliant

A2.1 Assessment Scope Does the scope of this assessment cover your whole organisation? Please note: Your organisation is only eligible for free Cyber Insurance if your assessment covers your whole company, if you answer "No" to this question you will not be invited to opt in to the included insurance. Your whole organisation includes all divisions, people and devices which access your organisation's data and services. About Scope Subset Scoping Guidance	Yes	Compliant
A2.3 Geographical Location Please describe the geographical locations of your business which are in the scope of this assessment. You should provide either a broad description (e.g. All UK offices) or simply list the locations in scope (e.g. Manchester and Glasgow retail stores).	All UK offices	Compliant

A2.4 End User Devices Please list the quantities and operating systems for your laptops, desktops and virtual desktops within the scope of this assessment. **Please Note: You must include make and operating system versions for all devices. All user devices declared within the scope of the certification only require the make and operating system to be listed. We have removed the requirement for you to list the model of the device.** **Devices that are connecting to cloud services must be included.** **A scope that does not include end user devices is not acceptable.** You need to provide a summary of all laptops, computers, virtual desktops and their operating systems that are used for accessing organisational data or services and have access to the internet. For example, “We have 25 DELL laptops running Windows 10 Professional version 22H2 and 10 MacBook laptops running MacOS Ventura"". Please note, the edition and feature version of your Windows operating systems are required. This applies to both your corporate and user owned devices (BYOD). You do not need to provide serial numbers, MAC addresses or further technical information. **Extended Security Update schemes** For any end-of-life operating system that has an extended security update program, you must maintain the required subscription. If you are using Windows 10 beyond the 14th October 2025 you must be signed up to the Microsoft Extended Security Update program in order to remain compliant. Further guidance: Operating System Support Guidance to BYOD	In each of our home offices, a single computer is used to access organisational data and services: 1. 14 Horn Street, Nunney, Frome, Somerset BA11 4NP: Windows 11 Professional Edition 24H2 Build 26100.6584 on an Asus Zenbook S16 laptop (AMD Ryzen AI 9 HX 370 w/ Radeon 890M 2.00 GHz, 32GB RAM) 2. Foxlowe House, Sherwood Road, Buxton, SK17 8HH: Windows 11 Professional Edition 24H2 Build 26100.6725 on a Scan desktop (AMD Ryzen 9 3950X 16-Core, 64GB RAM) 3. 4 Riding Cottages, Acomb, Hexham, NE46 4PF: Windows 11 Professional Edition 24H2 Build 26100.6584 on a custom-built PC (AMD Ryzen 5 3600x, 16GB RAM) on which the B450 GAMING PRO CARBON AC motherboard has BIOS version 7B85v1G (2022-07-29) installed, the latest production release available (https://pl.msi.com/Motherboard/B450-GAMING-PRO-CARBON-AC/support)	Compliant

A2.4.1 Thin Client Devices Please list the quantity of thin clients within the scope of this assessment. Please include make and operating systems. Please provide a summary of all the thin clients in scope that are connecting to organisational data or services (definitions of which are in the 'Cyber Essentials Requirements for IT Infrastructure' document linked in question A1.9). Thin clients are commonly used to connect to a Virtual Desktop Solution. Thin clients are a type of very simple computer holding only a base operating system which are often used to connect to virtual desktops. Thin clients can connect to the internet, and it is possible to modify some thin clients to operate more like PCs, and this can create security complications. Cyber Essentials requires thin clients to be supported and receiving security updates. Cyber Essentials Requirements for IT Infrastructure v3.2	None	Compliant
A2.5 Server Devices Please list the quantity of servers, virtual servers, virtual server hosts (hypervisors) and Virtual Desktop Infrastructure (VDI) servers. You must include the operating system. Please list the quantity of all servers within the scope of this assessment. For example: 2 x VMware ESXI 6.7 hosting 8 virtual Windows 2016 servers; 1 x MS Server 2019; 1 x Red Hat Enterprise Linux 8.3	None	Compliant

A2.6 Mobile Devices Please list the quantities of tablets and mobile devices within the scope of this assessment. Please Note: You must include make and operating system versions for all devices. All user devices within the scope of the certification only require the make and operating system to be listed. Devices that are connecting to cloud services must be included. A scope that does not include end user devices is not acceptable. Guidance to BYOD Operating System Support	Mobile devices used by our staff are used only for native voice / text / MFA applications and do not have access to organisational data or services, so our IASME assessor advises that they are out of scope for this assessment.	Compliant
A2.7 Networks Please provide a list of networks that will be in scope for this assessment. You should include details of each network used in your organisation including its name, location and its purpose (e.g. Main Network at Head Office for administrative use, Development Network at Malvern Office for testing software). You do not need to provide IP addresses or other technical information.	We work from 3 home offices, using routers supplied by our ISPs: Location: Head Office, Purpose: Administrative User 14 Horn Street, Nunney, Frome, Somerset BA11 4NP Location: UK Homeworkers, Purpose: Home workers network based in the UK Foxlowe House, Sherwood Road, Buxton, SK17 8HH 4 Riding Cottages, Acomb, Hexham, NE46 4PF The admin passwords for each router are changed from the default and maintained in compliance with our password policy. At each location, we use firewall and (where HTTPS and SSH are insufficient, e.g., over public or unsecured networks) VPN software to access organisational data and services. All such software is updated automatically, and the passwords are maintained in compliance with our password policy.	Compliant

A2.7.1 Home or remote workers How many staff are home or remote workers? Any employee that has been given permission to work remotely (for any period of time at the time of the assessment) needs to be classed as a home/remote worker for Cyber Essentials. For further guidance see the Home and remote working section in the Cyber Essentials Requirements for IT Infrastructure document. Cyber Essentials Requirements for IT Infrastructure v3.2	All our 3 staff work from their own home office: 1. Head Office (14 Horn Street, Nunney, Frome, Somerset BA11 4NP): Keith Harrison-Broninski (Chief Executive Officer) 2. UK Homeworker 1 (Foxlowe House, Sherwood Road, Buxton, SK17 8HH): Peter Lawrence (Chief Technology Officer) 3. UK Homeworker 2 (4 Riding Cottages, Acomb, Hexham, NE46 4PF): Alistair Revill (Software developer)	Compliant
A2.8 Network Equipment Please provide a list of network equipment that will be in scope for this assessment (including firewalls and routers). You must include make and model of each device listed. You should include all equipment that controls the flow of data to and from the internet. This will be your routers and firewalls. You do not need to include switches or wireless access points that do not contain a firewall or do not route internet traffic. If you have home and/or remote workers they will be relying on software firewalls, please describe in the notes field. You are not required to list any IP addresses, MAC addresses or serial numbers.	As per A2.7, Networks, we work from 3 home offices using routers supplied by our ISPs. These routers are all owned by homeworkers, so (as advised by our IASME assessor) only our head office network/location is shown below. Other homeworker owned routers are omitted are excluded from the scope as they rely on device software firewalls. Location: Head Office Purpose: Administrative User Address: Horn Street, Nunney, Frome, Somerset BA11 4NP Router: Zyxel VMG8825-T50K The admin passwords for all routers are changed from the default and maintained in compliance with our password policy. At each location, we use firewall and (where HTTPS and SSH are insufficient, e.g., over public or unsecured networks) VPN software to access organisational data and services. All such software is updated automatically, and the passwords are maintained in compliance with our password policy.	Compliant

A2.9 Cloud Services Please list all of the cloud services that are in use by your organisation and provided by a third party. **Please note that cloud services cannot be excluded from the scope of Cyber Essentials.** You need to include details of all of your cloud services. This includes all types of services - Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Definitions of the different types of cloud services are provided in the 'Cyber Essentials Requirements for IT Infrastructure' document. Cyber Essentials Requirements for IT Infrastructure v3.2	Google Cloud: 1. Artifact Registry 2. GCloud Run 3. GCloud FileStore	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.	Peter Lawrence Custom Fields: Responsible Person Role: Chief Technical Officer	Compliant
A3.1 Head Office Is your head office domiciled in the UK or Crown Dependencies and is your gross annual turnover less than £20m? This question relates to the eligibility of your organisation for the included cyber insurance.	Yes	Compliant
A3.2 Cyber Insurance If you have answered "yes" to the last question then your organisation is eligible for the included cyber insurance if you gain certification. If you do not want this insurance element please opt out here. There is no additional cost for the insurance. You can see more about it at https://iasme.co.uk/cyber-essentials/cyber-liability-insurance/	Opt-In	Compliant

A3.3 Insurance Contact What is the organisation email contact for the insurance documents? You only need to answer this question if you are taking the insurance. The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification and they will use this to contact you with your insurance documents and renewal information.	khb@collaboration-tools.com	Compliant
A4.1 Boundary Firewall Do you have firewalls at the boundaries between your organisation's internal networks, laptops, desktops, servers and the internet? You must have firewalls in place between your office network and the internet. **CE Requirement:** You must protect every device in scope with a correctly configured firewall (or network device with firewall functionality). Further guidance: Firewalls	Yes Custom Fields: Applicant Notes: All our devices including computers and mobile phones use firewall software to monitor and control incoming and outgoing network traffic. This software acts as a barrier between our devices and untrusted external networks, such as the internet, thus protecting against unauthorized access and other cyberthreats. Windows: Windows Firewall, https://learn.microsoft.com/en-us/windows/security/operatingsystem-security/network-security/windows-firewall Android: NetGuard, https://netguard.me All our devices including computers and mobile phones also use VPN software (a commercial product, not administered by our organisation) to create secure connections between our devices and the internet where HTTPS and SSH are insufficient, e.g., over public or unsecured networks. The VPN software encrypts our data and masks our IP addresses. Windows and Android: Proton VPN, https://protonvpn.com All software above is updated automatically, and the passwords are maintained in compliance with our password policy.	Compliant

A4.1.1 Off Network Firewalls Do you have software firewalls enabled on all of your computers, laptops and servers? Your software firewall needs to be configured and enabled at all times, even when sitting behind a physical/virtual boundary firewall in an office location. Guidance on how to check your software firewall can be found here: About Firewalls **CE Requirement:** You must protect every device in scope with a correctly configured firewall (or network device with firewall functionality). **CE Requirement:** Make sure you use a software firewall on devices which are used on untrusted networks, such as public wifi hotspots. If your organisation doesn't control the network to which a device connects, you must configure a software firewall on the device.	Yes	Compliant
A4.2 Firewall Default Password When you first receive an internet router or hardware firewall device, it may have had a default password on it. Have you changed all the default passwords on your boundary firewall devices? The default administrator password must be changed on all routers and firewalls, including those that come with a unique password pre-configured (e.g. BT Business Hub, Draytek Vigor 2865ac). When relying on software firewalls included as part of the operating system of your end user devices, the password to access the device will need to be changed. **CE Requirement:** Change default administrative passwords to a strong and unique password – or disable remote administrative access entirely. Further guidance: About Routers	Yes Custom Fields: Applicant Notes: The default password on each of our routers is changed on installation and maintained in compliance with our password policy.	Compliant

A4.2.1 Firewall Password Change Process Please describe the process for changing your firewall password. Home routers not supplied by your organisation are not included in this requirement. You need to understand how the password on your firewall(s) is changed. Please provide a brief description of how this is achieved.	We currently work from home offices, using home routers supplied by our ISPs. These are not supplied by us, so our IASME assessor advises that they are not included in this requirement. As per A4.1, all our devices including computers and mobile phones use software firewalls to access organisational data and services. Computers (all Windows): Windows Firewall, https://learn.microsoft.com/en-us/windows/security/oper ating-system-security/network-security/windows-firewall 1. Windows Firewall does not have an applicationspecific password - rather, Windows Firewall settings are managed via an operating system account with administrative privileges. 2. To change the password of an administrator account in Windows: 2.1 Press Windows + I to open Settings. 2.2 In the Settings window, click on Accounts. 2.3 In the left sidebar, select Sign-in options. 2.4 Under the Password section, click on Change. 2.5 To change the password, enter the current password (if set) then enter a new password, adhering strictly to our password policy 2.6 Save the New Password 3. Note that we require the use of separate accounts for administrative tasks, ensuring that employees use a standard user account for everyday use and a separate administrator account solely for performing administrative tasks (such as adjusting settings in Windows Firewall). Mobile phones (all Android): NetGuard: https://netguard.me 1. Open the NetGuard App 2. In the main screen, tap on the three vertical dots in the top-right corner to open the menu 3. From the dropdown menu, select Settings 4. In the Settings menu, scroll down to find the Password section 5. To change the password, enter the current password (if set) then enter a new password, adhering strictly to our password policy 6. Confirm the new password by entering it again 7. Save changes	Compliant

A4.3 Firewall Password Configuration How is your firewall password configured? Please select the options being used: A. Multi-factor authentication, with a minimum password length 8 characters and no maximum length B. Automatic blocking of common passwords, with a minimum password length 8 characters and no maximum length C. A password minimum length of 12 characters and no maximum length D. Passwordless system is being used as an alternative to user name and password, please describe E. None of the above, please describe Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the section about password-based authentication in the 'Cyber Essentials Requirements for IT Infrastructure' document. Cyber Essentials Requirements for IT Infrastructure v3.2 **CE Requirement:** Prevent access to the administrative interface (used to manage firewall configuration) from the internet, unless there is a clear and documented business need, and the interface is protected by one of the following controls: • multi-factor authentication • an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach Further guidance : Bulletproof your passwords	0: A. Multi-factor authentication, with a minimum password length 8 characters and no maximum length, 1: B. Automatic blocking of common passwords, with a minimum password length 8 characters and no maximum length, 2: C. A password minimum length of 12 characters and no maximum length Custom Fields: Applicant Notes: The local admin password for the firewall application on each device is configured as per our password policy: 1. At least 12 characters in length 2. A mixture of letters, cases, numbers, and symbols 3. Generated by a password manager to avoid accidental use of common passwords Note that master passwords for password managers are: 1. Created from 3 random words, capitalised in places and with numbers substituted for some letters. 2. Committed to memory. Multi-Factor Authentication is required to access software firewalls and password managers.	Compliant

A4.4 Firewall Password Issue Do you change your firewall password when you know or suspect it has been compromised? Passwords may be compromised if there has been a virus on your system or if the manufacturer notifies you of a security weakness in their product. You should be aware of this and know how to change the password if this occurs. When relying on software firewalls included as part of the operating system of your end user devices, the password to access the device will need to be changed. **CE Requirement:** You should make sure there is an established process in place to change passwords promptly if you know or suspect a password or account has been compromised. Further guidance: Compromised Accounts	Yes	Compliant
A4.5 Firewall Management Process Do you have a process to manage your firewall? At times your firewall may be configured to allow a system on the inside to become accessible from the internet (for example: a VPN server, a mail server, an FTP server, or a service that is accessed by your customers). This is sometimes referred to as "opening a port". You need to show a business case for doing this because it can present security risks.	Yes Custom Fields: Applicant Notes: Scope: 1. All our services are hosted on the Google Cloud Platform (GCP) environment - we have no other services, local or otherwise. 2. All network access control is implemented and enforced through Google Cloud Virtual Private Cloud (VPC) firewall rules, managed centrally by the CTO. 3. All boundary protection, network segregation, and access control are implemented using GCP-native firewall services, under the governance of our centralised cloud security management framework. 4. We maintain a formal process for the management, configuration, and review of firewalls within GCP. 5. The firewall management process is governed by the organisations Network Security Policy and adheres to the principles of least privilege and business justification for external exposure. Firewall Configuration and Change Control: 1. Firewall rules are configured to deny all inbound connections by default. 2. Any requirement to allow external	Compliant

	access (e.g., HTTPS, VPN, or other public-facing services) must be supported by a documented business case outlining operational necessity and associated security considerations. 3. All requests for new or amended firewall rules follow a formal change management process, including: 3.1. Submission of a change request via the internal change control system. 3.2. Security assessment by the CTO to validate justification and ensure compliance with organisational policy. 3.3. Approval and implementation by authorised personnel only. 3.4. Logging and version control of all firewall configuration changes. Ongoing Management and Review: 1. Firewall rules and configurations are reviewed at least quarterly, or sooner if there is a significant infrastructure or service change. 2. Temporary or exceptional access rules are configured with expiry dates and are removed once no longer required. 3. All firewall activities are monitored and logged using Google Cloud Logging and Security Command Center to detect unauthorised access or configuration changes. 4. Alerts are configured to notify the CTO of any critical changes or potential policy violations.	
A4.6 Firewall Review Process Have you reviewed your firewall rules in the last 12 months? Please describe your review process. If you no longer need a service to be enabled on your firewall, you must remove it to reduce the risk of compromise. You should have a process that you follow to do this (i.e. when are services reviewed, who decides to remove the services, who checks that it has been done?). **CE Requirement:** Remove or disable inbound firewall rules quickly when they are no longer needed.	Yes, our firewall rules have been reviewed within the last 12 months. Context: 1. Our organization hosts all services exclusively within Google Cloud Platform (GCP). 2. Firewall management is handled through Google Clouds VPC Firewall Rules and associated Security Command Center and IAM policies. 3. We have an established review and change management process to ensure only required services and ports are exposed, described below. Review Frequency: Firewall rules are reviewed at least quarterly as part of our cloud security maintenance schedule, and additionally during any major infrastructure or service change. Responsibility: The CTO (or delegated Cloud Administrator) is responsible for reviewing and approving all firewall rule changes. The review includes checking	Compliant

	for any obsolete or overly permissive rules. Review Process: 1. GCP firewall rules are exported and reviewed for compliance against our baseline security policy. 2. Each rule is checked for necessity, source/destination restrictions, and exposure of sensitive services. 3. Any rule not justified by a current business requirement is marked for removal. Change Control and Removal: 1. Once a rule is identified as no longer required, it is removed immediately via the GCP console or IaC (Infrastructure as Code) pipeline. 2. The CTO verifies removal and logs the change in our Change Management Register for audit purposes. Monitoring and Alerts: GCPs Security Command Center and Cloud Logging provide ongoing visibility into firewall configuration changes and trigger alerts for unauthorized modifications. Summary: 1. Firewall rules in GCP are reviewed and updated at least quarterly to ensure compliance with the Cyber Essentials requirement. 2. Any unneeded inbound rules are removed promptly to minimize exposure and reduce the risk of compromise.	
A4.7 Firewall Inbound Connections Is your firewall configured to allow unauthenticated inbound connections? By default, most firewalls block all services inside the network from being accessed from the internet, but you need to check your firewall settings. **CE Requirement:** Block unauthenticated inbound connections by default.	No	Compliant

A4.8 Allowed Connections Please describe how you approve and document your allowed inbound connections. The business case should be documented and recorded. A business case must be signed off at board level and associated risks reviewed regularly. At times your firewall may be configured to allow a system on the inside to become accessible from the internet (for example: a VPN server, a mail server, an FTP server, or a service that is accessed by your customers). This is sometimes referred to as "opening a port". You need to show a business case for doing this because it can present security risks. **CE Requirement:** Ensure inbound firewall rules are approved and documented by an authorised person, and include the business need in the documentation.	All inbound connections are managed and controlled through Google Cloud Firewall Policies within our Google Cloud Platform (GCP) environment. Inbound firewall rules are created only when there is a documented business need, approved by the CTO and reviewed by the Board as part of our regular risk assessment process. Firewall rules are reviewed at least quarterly and immediately removed or disabled when access is no longer required. All inbound firewall rules are recorded in our Change Management and Access Control Register with: 1. Description of the business case 2. Associated risk assessment 3. Authorised approver (by default, the CTO) 4. Date of approval 5. Configuration 6. Review schedule, if more than quarterly	Compliant

A4.9 Firewall Remote Configuration Are your boundary firewalls configured to allow access to their configuration settings over the internet? Sometimes organisations configure their firewall to allow other people (such as an IT support company) to change the settings via the internet. If you have not set up your firewalls to be accessible to people outside your organisations or your device configuration settings are only accessible via a VPN connection, then answer "no" to this question. **CE Requirement:** Prevent access to the administrative interface (used to manage firewall configuration) from the internet, unless there is a clear and documented business need, and the interface is protected by one of the following controls: • multi-factor authentication • an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach Guidance on VPNs	No	Compliant

A5.1 Remove Unused Software Have you removed or disabled software and services that you do not use on your laptops, desktop computers, thin clients, servers, tablets, mobile phones and cloud services? Describe how you achieve this. You must remove or disable applications, system utilities and network services that are not needed in day-to-day use. You need to check your cloud services and disable any services that are not required for day-to-day use. To view installed applications: Windows: Right-click on Start > Apps and Features macOS: Open Finder > Applications Linux: Open your software package manager (apt, rpm, yum) **CE Requirement:** You must regularly remove or disable unnecessary software (including applications, system utilities and network services). Further guidance : Removing unnecessary software	To ensure the security of our devices and cloud services, we have a comprehensive process to remove or disable all software and services that are not needed for our day-to-day operations. The process is based on a regular audits of installed software and services to ensure compliance with our security policy and identify any new software / services that can be disabled / removed: 1. Inventory Assessment: We regularly conduct a detailed assessment of all software installed on our laptops, desktop computers, and mobile phones. This generates a list of all applications currently in use across our organization. 2. Usage Analysis: We analyse this list to determine which applications are essential for our daily operations and which are redundant or unused. 3. Deactivation and Removal: For applications identified as unnecessary, we either uninstall or disable them. Where applicable, this is done using automated scripts and software management tools. 4. Cloud Services (GCloud only at present) Review: We regularly review our subscriptions and settings for cloud services to ensure that only necessary services are active. Unused or redundant cloud services are disabled or unsubscribed. 5. Security Protocol: Our security protocol disallows the installation of software or purchase of cloud services without authorization from senior management. 6. Documentation: All actions and processes undertaken are documented for accountability and reference. 7. Training: New employees receive training on our security practices, including the importance of minimizing software and services usage. This process applies to devices including Desktop Computers, Laptops, and Mobile Phones as well as to cloud services including IaaS, PaaS and SaaS. We do not use Servers, Tablets, or Thin Clients.	Compliant

A5.2 Remove Unrequired User Accounts Have you ensured that all your laptops, computers, servers, tablets, mobile devices and cloud services only contain necessary user accounts that are regularly used in the course of your business? You must remove or disable any user accounts that are not needed in day-to-day use on all devices and cloud services. To view user accounts: Windows: Right-click on Start > Computer Management > Users macOS: System Settings > Users and Groups Linux: "cat/etc/passwd" **CE Requirement:** You must regularly remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used).	Yes	Compliant

A5.3 Change Default Password Have you changed the default password for all user and administrator accounts on all your desktop computers, laptops, thin clients, servers, tablets and mobile phones that follow the Password-based authentication requirements of Cyber Essentials? A password that is difficult to guess will be unique and not be made up of common or predictable words such as "password" or "admin", or include predictable number sequences such as "12345". **CE Requirement:** You must regularly change any default or guessable account passwords. Use technical controls to manage the quality of passwords. This will include one of the following: • using multi-factor authentication • a minimum password length of at least 12 characters, with no maximum length restrictions • a minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list	Yes	Compliant
A5.4 Internally hosted External Services Do you run or host external services that provide access to data (that shouldn't be made public) to users across the internet? Your business might run software that allows staff or customers to access information across the internet to an external service hosted on the internal network, cloud data centre or IaaS cloud service. This could be a VPN server, a mail server, or an internally hosted internet application such as a SaaS or PaaS cloud service that you provide to your customers as a product. In all cases, these applications provide information that is confidential to your business and your customers and that you would not want to be publicly accessible. **CE Requirement:** Ensure users are authenticated before allowing them access to organisational data or services.	No	Compliant

A5.8 Auto-run Disabled Have you disabled any feature which allows automatic file execution of downloaded or imported files without user authorisation? This is a setting on your device which automatically runs software on external media or downloaded from the internet. It is acceptable to choose the option where a user is prompted to make a choice about what action will occur each time they insert a memory stick. If you have chosen this option, you can answer yes to this question. **CE Requirement:** Disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded).	Yes	Compliant
A5.9 Device Unlocking When a device requires a user to have the device in hand, do you set a locking mechanism on your devices to access the software and services installed? Device locking mechanisms such as biometric, password or PIN, need to be enabled to prevent unauthorised access to devices accessing organisational data or services. **CE Requirement:** Ensure appropriate device locking controls for users that are physically present.	Yes Custom Fields: Applicant Notes: Devices are unlocked using a PIN (6 character minimum) or biometrics.	Compliant

A5.10 Device Unlocking Method Which method do you use to unlock the devices? Please refer to Device Unlocking Credentials paragraph found under Secure Configuration in the Cyber Essentials Requirements for IT Infrastructure document for further information. Cyber Essentials Requirements for IT Infrastructure v3.2 The use of a PIN with a length of at least six characters can only be used where the credentials are just to unlock a device and does not provide access to organisational data and services without further authentication. **CE Requirement:** If a device requires a user's physical presence to access a device's services (such as logging on to a laptop or unlocking a mobile phone), a credential such as a biometric, password or PIN must be in place before a user can gain access to the services. You must protect your chosen authentication method against brute-force attacks. When it's possible to configure, you should apply one of the following: • 'throttling' the rate of attempts, so that the length of time the user must wait between attempts increases with each unsuccessful attempt - you shouldn't allow more than 10 guesses in 5 minutes • locking devices after more than 10 unsuccessful attempts • When the vendor doesn't allow you to configure the above, use the vendor's default setting.	Our desktop and mobile devices are unlocked with a biometric test and / or a PIN of minimum length six characters. Further authentication is then required to access software and services providing access to organizational data: 1. Passwords, created and maintained in compliance with our password policy 2. Where the software / service enables it, multi-factor authentication to confirm user identity	Compliant

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

A6.2 Supported software Is all the software on your devices supported by a supplier that produces regular vulnerability fixes for any security problems? All software used by your organisation must be supported by a supplier who provides regular security updates and vulnerability fixes. Unsupported software must be removed from your devices. This includes frameworks and extensions. **CE Requirement:** You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	Yes	Compliant
A6.2.1 Internet Browsers Please list your internet browser(s). The version is required. Please list all internet browsers installed on your devices, so that the Assessor can understand your setup and verify that they are in support. For example: Chrome Version 124, Safari Version 15. **CE Requirement:** You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	Google Chrome, Version 141.0.7390.108 (Official build) (64-bit) Microsoft Edge, Version 141.0.3537.71 (Official build) (64-bit) Mozilla Firefox, Version144.0 (64-bit)	Compliant
A6.2.2 Malware Protection Please list your malware protection software The version is required. Please list all malware protection and versions you use so that the Assessor can understand your setup and verify that they are in support. For example: Sophos Endpoint Protection V10, Microsoft Defender, Bitdefender Internet Security 2023. **CE Requirement:** You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	Windows Defender (all locations): Security intelligence version: 1.439.141.0 Engine version: 1.1.25090.3001 Platform (core) version: 4.18.25080.5	Compliant

A6.2.3 Email Applications Please list your email applications installed on end user devices and server. The version is required. Please list all email applications and versions you use so that the Assessor can understand your setup and verify that they are in support. For example: MS Exchange 2016, Outlook 2019. **CE Requirement:** You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	Google Mail, via the Web interface only (not via a downloaded client application)	Compliant
A6.2.4 Office Applications Please list all office applications that are used to create organisational data. The version is required. Please list all office applications and versions you use so that the Assessor can understand your setup and verify that they are in support. For example: MS 365, Libre Office, Google Workspace, Office 2016. **CE Requirement**: You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.	HQ: Microsoft® Word LTSC MSO (Version 2408 Build 16.0.17932.20540) 64-bit, Microsoft® PowerPoint® LTSC MSO (Version 2408 Build 16.0.17932.20540) 64-bit, Microsoft® Excel® LTSC MSO (Version 2408 Build 16.0.17932.20540) 64-bit Other Locations: Microsoft® 365 (Current Channel - currently the October 7, 2025 release Version 2509, Build 19231.20172) - Word, Excel, and PowerPoint only All locations: Google Workspace	Compliant
A6.3 Software Licensing Are any of the in-scope software or cloud services unlicensed or unsupported? All software must be licensed. It is acceptable to use free and open-source software as long as you comply with any licensing requirements. Please be aware that for some operating systems, firmware and applications, if annual licensing is not purchased, they will not be receiving regular security updates. **CE Requirement:** All software on in-scope devices must be licensed and supported.	No	Compliant

A6.4 Security Updates - Operating System Are all high-risk or critical security updates and vulnerability fixes for operating systems and router and firewall firmware installed within 14 days of release? You must install all high and critical security updates and vulnerability fixes within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question. You are not required to install feature updates or optional updates in order to meet this requirement. This requirement includes the firmware on your firewalls and routers. **CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where: • The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk' • The update addresses vulnerabilities with a CVSSv3 base score of 7 or above • There are no details of the level of vulnerabilities the update fixes provided by the vendor Please note: For optimum security we strongly recommend (but it's not mandatory) that all released updates are applied within 14 days of release. It's important that updates are applied as soon as possible. 14 days is considered a reasonable period to be able to implement this requirement. Any longer would constitute a serious security risk while a shorter period may not be practical.	Yes	Compliant
A6.4.1 Auto-Updates - Operating System Are all updates applied for operating systems by enabling auto updates? Most devices have the option to enable auto updates. This must be enabled on any device where possible. **CE Requirement**: All software on in-scope devices must have automatic updates enabled where possible.	Yes	Compliant

A6.4.2 Manual Updates - Operating System Where auto updates are not being used, how do you ensure all high-risk or critical security updates and vulnerability fixes of all operating systems and firmware on firewalls and routers are applied within 14 days of release? It is not always possible to apply auto updates, this is often the case when you have critical systems or servers and you need to be in control of the updating process. Please describe how any updates are applied when auto updates are not configured. If you only use auto updates, please confirm this in the notes field for this question. **CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where: • The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk' • The update addresses vulnerabilities with a CVSSv3 base score of 7 or above • There are no details of the level of vulnerabilities the update fixes provided by the vendor	Where possible, our operating system software is automatically updated as soon as new versions become available. When auto updates are not possible (for example, in production environments where functionality may be affected), we use the following process to ensure all high-risk or critical security updates are applied within 14 days of release: 1. Monitoring: We monitor notifications from trusted sources such as vendor bulletins, cybersecurity newsletters, and vulnerability databases to stay informed about new updates and patches as they are released. 2. Assessment and Prioritization: Upon the release of an update, we assess its relevance and criticality to our systems using a risk-based approach. High-risk vulnerabilities are prioritized for immediate action. 3. Staging Environment Testing: If possible, before applying updates to production systems, we test them in a controlled staging environment to ensure that they do not disrupt critical operations and to verify compatibility with existing applications and hardware. 4. Scheduled Application: Once approved, updates are scheduled for deployment during off-peak hours to reduce impact on operations. We prioritize the application of updates based on the severity of the risk they mitigate. 5. Implementation: Updates are applied to all impacted systems, starting with the most vulnerable or business-critical systems and following a strict protocol to ensure all systems are uniformly updated. This is done through a central management console where available. 6. Verification: Post-update, we conduct verification checks to confirm that the updates have been successfully applied and systems are functioning as expected. 7. Documentation: Detailed records of each update cycle are documented for auditing and compliance purposes. This includes recording the date of the update, the systems affected, and verification results.	Compliant

A6.5 Security Updates - Applications Are all high-risk or critical security updates and vulnerability fixes for applications (including any associated files and extensions) installed within 14 days of release? You must install any such updates and vulnerability fixes within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question. You are not required to install feature updates or optional updates in order to meet this requirement, just high-risk or critical security updates. **CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where: • The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk' • The update addresses vulnerabilities with a CVSSv3 base score of 7 or above • There are no details of the level of vulnerabilities the update fixes provided by the vendor	Yes Custom Fields: Applicant Notes: Where possible, our application software is automatically updated with all security updates as soon as they become available. When auto updates are not possible (for example, in production environments where functionality may be affected), we use the following process to ensure all high-risk or critical security updates are applied within 14 days of release: 1. Monitoring: We monitor notifications from trusted sources such as vendor bulletins, cybersecurity newsletters, and vulnerability databases to stay informed about new updates and patches as they are released. 2. Assessment and Prioritization: Upon the release of an update, we assess its relevance and criticality to our systems using a risk-based approach. High-risk vulnerabilities are prioritized for immediate action. 3. Staging Environment Testing: If possible, before applying updates to production systems, we test them in a controlled staging environment to ensure that they do not disrupt critical operations and to verify compatibility with existing applications and hardware. 4. Scheduled Application: Once approved, updates are scheduled for deployment during off-peak hours to reduce impact on operations. We prioritize the application of updates based on the severity of the risk they mitigate. 5. Implementation: Updates are applied to all impacted systems, starting with the most vulnerable or business-critical systems and following a strict protocol to ensure all systems are uniformly updated. This is done through a central management console where available. 6. Verification: Post-update, we conduct verification checks to confirm that the updates have been successfully applied and systems are functioning as expected. 7. Documentation: Detailed records of each update cycle are documented for auditing and compliance purposes. This includes recording the date of the update, the systems affected, and verification results.	Compliant

A6.5.1 Auto-updates- Applications Are all updates applied on your applications by enabling auto updates? Most devices have the option to enable auto updates. Auto updates should be enabled where possible. **CE Requirement:** All software on in-scope devices must have automatic updates enabled where possible.	Yes Custom Fields: Applicant Notes: Where software supports this, except for production environments	Compliant

A6.5.2 Manual Updates - Applications Where auto updates are not being used, how do you ensure all high-risk or critical security updates and vulnerability fixes of all applications are applied within 14 days of release? It is not always possible to apply auto updates, this is often the case when you have critical systems or applications and you need to be in control of the updating process. Please describe how any updates and vulnerability fixes are applied when auto updates are not configured. If you only use auto updates, please confirm this in the notes field for this question. **CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where: • The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk' • The update addresses vulnerabilities with a CVSSv3 base score of 7 or above • There are no details of the level of vulnerabilities the update fixes provided by the vendor	Where possible, our application software is automatically updated as soon as new versions become available. When auto updates are not possible (for example, in production environments where functionality may be affected), we use the following process to ensure all high-risk or critical security updates are applied within 14 days of release: 1. Monitoring: We monitor notifications from trusted sources such as vendor bulletins, cybersecurity newsletters, and vulnerability databases to stay informed about new updates and patches as they are released. 2. Assessment and Prioritization: Upon the release of an update, we assess its relevance and criticality to our systems using a risk-based approach. High-risk vulnerabilities are prioritized for immediate action. 3. Staging Environment Testing: If possible, before applying updates to production systems, we test them in a controlled staging environment to ensure that they do not disrupt critical operations and to verify compatibility with existing applications and hardware. 4. Scheduled Application: Once approved, updates are scheduled for deployment during off-peak hours to reduce impact on operations. We prioritize the application of updates based on the severity of the risk they mitigate. 5. Implementation: Updates are applied to all impacted systems, starting with the most vulnerable or business-critical systems and following a strict protocol to ensure all systems are uniformly updated. This is done through a central management console where available. 6. Verification: Post-update, we conduct verification checks to confirm that the updates have been successfully applied and systems are functioning as expected. 7. Documentation: Detailed records of each update cycle are documented for auditing and compliance purposes. This includes recording the date of the update, the systems affected, and verification results.	Compliant

A6.6 Unsupported Software Removal Have you removed any software installed on your devices that is no longer supported and no longer receives regular updates or vulnerability fixes for security problems? You must remove older software from your devices when it is no longer supported by the manufacturer. Such software might include older versions of web browsers, operating systems, and all application software. **CE Requirement**: All software on in-scope devices must be removed from devices when it becomes unsupported, or removed from scope by using a defined sub-set that prevents all traffic to/from the internet.	Yes	Compliant
A6.7 Unsupported Software Segregation Where you have a business need to use unsupported software, have you moved the devices and software out of scope of this assessment? Please explain how you achieve this. Software that is not removed from devices when it becomes un-supported will need to be placed onto its own sub-set with no internet access. If the out-of-scope sub-set remains connected to the internet, you will not be able to achieve whole company certification and an excluding statement will be required in question A2.2. A sub-set is defined as a part of the organisation whose network is segregated from the rest of the organisation by a firewall or VLAN. Where no unsupported software is used across your whole organisation, please declare this here. **CE Requirement**: All software on in-scope devices must be removed from devices when it becomes unsupported, or removed from scope by using a defined sub-set that prevents all traffic to/from the internet. Further guidance: Subset Scoping Guidance	We only deploy and use supported software. Where software is scheduled to go out of support, we transition away from the software beforehand to an alternative for which support is available, using the following process: 1. Monitoring: We monitor end-of-support notifications from the vendors of all our software 2. Assessment and Prioritization: When software is announced as going out of support, we determine the functionality required and identify suitable alternative software. 3. Staging Environment Testing: We test the alternative software in a controlled staging environment to ensure that it does not disrupt critical operations and to verify compatibility with existing applications and hardware. 4. Scheduled Replacement: Once testing has concluded successfully, removal of the old software and installation of the alternative is scheduled for deployment during off-peak hours to reduce impact on operations. 5. Verification: Post-replacement, we conduct verification checks to confirm that the old software has been fully removed, the new software has been successfully installed, and all systems continue to function as expected. 6. Documentation: We update our records to show replacement of the old software with the new software on all affected devices.	Compliant

A7.1 User Account Creation Are your users only provided with user accounts after a process has been followed to approve their creation? Describe the process. You must ensure that user accounts (such as logins to laptops and accounts on servers) are only provided after they have been approved by a person with a leadership role in the business. **CE Requirement:** Your organisation must have in place a process to create and approve user accounts.	The only cloud services we use are GCloud and Google Workspace, for which only the administrators (Chief Technical Officer Peter Lawrence and Chief Executive Officer Keith Harrison-Broninski) can approve access. Access is restricted to company employees. We use a structured process in place to monitor and approve the usage of Desktop Computers, Laptops, and Mobile Phones to access organisational data and services: 1. Request Submission: A formal request for access must be submitted. 2. Managerial Approval: The request is then reviewed and must be approved to ensure that there is a legitimate business need for the access. 3. Access Level Determination: Based on the review, the appropriate access level is determined based on the principle of least privilege (i.e., the user will only receive the access necessary to perform their job functions). 4. Access Enablement: After approval, we ensure that the device is used in accordance with company protocols, such as mandatory use of firewall / VPN software, compliance with our password policy, and automatic updates to software. 5. Access Logging: Use of the device is recorded to ensure accountability and traceability/ We use no Servers, Tablets, or Thin Clients.	Compliant
A7.2 Unique Credentials Are all your user and administrative accounts accessed by entering unique credentials? You must ensure that no devices, applications or cloud services can be accessed without entering unique access credentials. Accounts must not be shared. **CE Requirement:** Authenticate users with unique credentials before granting access to applications or devices.	Yes	Compliant

A7.3 Leaver Accounts How do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation? When an individual leaves your organisation, you need to stop them accessing any of your systems. **CE Requirement:** Remove or disable user accounts when no longer required.	We manage leaver accounts as follows: 1. Access Review: Following the advance notification of an employees departure, which typically happens as soon as the resignation or termination is confirmed, we review the departing employees access privileges across all systems, applications, and data repositories to identify all accounts and access to data / services associated with the individual. 2. Account Disablement: On or before the employees last working day, all system access is either disabled or deleted. This includes network login credentials, email accounts, remote access privileges, any application-specific accounts, and removal from cloud services (GCloud and Google Workspace). Prior to disabling accounts, we review access logs to ensure there was no unusual activity. Accounts are then disabled. 3. Account Deletion: Following account disablement, we verify that all necessary access has been revoked and provide approval for account deletion. After a set retention period to ensure no essential data is needed from the accounts, they are permanently deleted. 4. Account Audit: We conduct regular audits of user accounts to ensure that there are no active accounts for individuals no longer associated with the organization.	Compliant

A7.4 User Privileges Do you ensure that staff only have the access privileges that they need to do their current job? How do you do this? When a staff member changes job role you may also need to change their permissions to only access the files, folders and applications that they need to do their day-to-day work. For Cyber Essentials we require that the principle of least privilege be applied. **CE Requirement**: Your organisation must be in control of your user accounts and the access privileges that allow access to your organisational data and services.	Currently we only have two senior managers both with full privileges and a software developer with limited privileges. As the company grows, we continue to ensure that staff only have the privileges they need to perform their current job responsibilities as follows: 1. Role-Based Access Control (RBAC): Access permissions are based on the users role within the organization, so that each employee only has access to the files, folders, and applications necessary for their specific job functions. 2. Access Reviews: We conduct regular audits of user access rights to verify that permissions are aligned with current job responsibilities, ensuring that no employee retains access that has become unnecessary or is lacking access that they now need. 3. Access Requests: Any changes to user privileges require formal approval by senior managers, who verify the necessity for additional access privileges based on the users job role. 4. Onboarding and Offboarding: During onboarding, senior managers assign access based on the employees role. Offboarding is done as per the leaver process described above, under which access to all data and services is revoked. 5. Role Change: When an employee changes job role, senior managers reassess their access needs and adjust permissions accordingly, consulting with the employee to ensure they have appropriate and necessary access levels.	Compliant

A7.5 Administrator Approval Do you have a formal process for giving someone access to systems at an “administrator” level and can you describe this process? You must have a process that you follow when deciding to give someone access to systems at administrator level. This process might include approval by a person who is an owner/director/trustee/partner of the organisation. **CE Requirement:** Your organisation must have in place a process to create and approve user accounts.	To control administrator level access to our systems, we extend the generic access control process as described in the sub-bullets below: 1. Role-Based Access Control (RBAC): Access permissions are based on the users role within the organization, so that each employee only has access to the files, folders, and applications necessary for their specific job functions. 1.1 Before granting administrator access, a clear justification must be provided outlining the necessity of administrator privileges for the individuals role or project requirements. 2. Access Reviews: We conduct regular audits of user access rights to verify that permissions are aligned with current job responsibilities, ensuring that no employee retains access that has become unnecessary or is lacking access that they now need. 2.1 Administrator activities are routinely monitored for any unusual or unauthorized actions. Access permissions are reviewed periodically, and adjustments are made as necessary to maintain security and efficiency. 3. Access Requests: Any changes to user privileges require formal approval by senior managers, who verify the necessity for additional access privileges based on the users job role. 3.1. Administrator access requires a formal access request detailing the specific systems for which administrator access is needed, the duration of access required, and the business justification. 3.2. This request is reviewed by the CTO to evaluate the necessity and potential risks associated with granting access. 3.3. If the request is approved, the individual must sign an administrator access agreement, acknowledging understanding and compliance with the organizations IT security policies and procedures. 3.4. Upon completion of the project (or termination of the individuals employment), administrator access is promptly revoked. 4. Onboarding and Offboarding: During onboarding, senior managers assign access based on the employees role. Offboarding is done as per the leaver process described above, under which access to all data and services is revoked. 5. Role Change: When an employee changes job role, senior managers reassess their access needs and adjust permissions accordingly, consulting with the employee to ensure they have appropriate and necessary access levels.	Compliant

A7.6 Use of Administrator Accounts How does your organisation make sure that separate accounts are used to carry out administrative tasks (such as installing software or making configuration changes)? You must use a separate administrator account from the standard user account, when carrying out administrative tasks such as installing software. Using administrator accounts all day long exposes the device to compromise by malware. Cloud service administration must be carried out using separate accounts. Further guidance : User Access - Just Enough or Just In Time **CE Requirement:** Your organisation must use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks).	We enforce the use of separate accounts for administrative tasks by ensuring that employees use a standard user account for everyday use and a separate administrator account solely for performing administrative tasks. Administrative accounts are monitored to ensure they are only used when necessary, such as for installing software or making configuration changes. To prevent the misuse of administrator accounts, we have implemented the following measures: 1. Role-Based Access Control: Administrator accounts are assigned based on job roles and responsibilities, ensuring only authorised personnel have administrative privileges. 2. Multi-Factor Authentication : Access to administrator accounts requires at least 2 forms of verification, enhancing security against unauthorised access. 3. Session Monitoring & Auditing: All administrative actions and sessions are logged and regularly audited so that we detect and respond promptly to any suspicious activities. 4. Cloud Service Administration: Similar principles are applied to cloud services, where administrative tasks are handled through separate administrator accounts with restrictions that prevent use of personal or standard user accounts. Temporary Administrator Privileges are never granted.	Compliant

A7.7 Managing Administrator Account Usage How does your organisation prevent administrator accounts from being used to carry out everyday tasks like browsing the web or accessing email? This question relates to the activities carried out when an administrator account is in use. You must ensure that administrator accounts are not used to access websites or download email. Using such accounts in this way exposes the device to compromise by malware. Software and update downloads should be performed as a standard user and then installed as an administrator. You may not need a technical solution to achieve this, it could be based on good policy, procedure and regular training for staff. **CE Requirement:** Your organisation must use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks).	We use a multi-layered approach to prevent administrator accounts from being used for everyday tasks like browsing the web or accessing email. 1. Policy and Procedure: We have a strict policy in place that states administrator accounts are to be used solely for maintenance and administrative tasks and are prohibited from accessing email or browsing the web. This policy is communicated to all employees during onboarding and reiterated in updates to training. 2. Role-Based Access Control (RBAC): We use RBAC to ensure that users have the minimum level of access necessary for their job functions. Administrator privileges are only granted to select individuals, and only for specific tasks as necessary. 3. Separate User Accounts: All users, including administrators, have separate non-administrative accounts for everyday activities. This ensures browsing and email access are conducted through standard user privilege, reducing the risk of malware infection through high-privileged accounts. 4. Technical Controls: We employ technical controls such as Group Policy Objects (GPOs) in Windows environments and security alerts in Google Workspace to restrict administrative account usage to specific, approved applications and tools, preventing them from launching web browsers or email clients. 5. Monitoring and Auditing: We routinely audit the use of administrator accounts to ensure compliance with the above protocols. 6. Regular Training: To reinforce the importance of adhering to the established protocols and educate staff on the risks associated with improper administrative account use, we conduct annual training sessions along with intermediate training updates.	Compliant
A7.8 Administrator Account Tracking Do you formally track which users have administrator accounts in your organisation? You must track all people that have been granted administrator accounts. **CE Requirement:** Your organisation must have in place a process to create and approve user accounts.	Yes	Compliant

A7.9 Administrator Access Review Do you review who should have administrative access on a regular basis? You must review the list of people with administrator access regularly. Depending on your business, this might be monthly, quarterly or annually. Any users who no longer need administrative access to carry out their role should have it removed. **CE Requirement:** Your organisation must remove or disable special access privileges when no longer required (when a member of staff changes role, for example).	Yes	Compliant
A7.10 Brute Force Attack Protection Where you have systems that require passwords (or where passwords are a backup for a passwordless system), how are they protected from brute-force attacks? A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works. Information on how to protect against brute-force password guessing can be found in the Password-based authentication section, under the User Access Control section in the 'Cyber Essentials Requirements for IT Infrastructure' document. Cyber Essentials Requirements for IT Infrastructure v3.2 **CE Requirement**: Passwords are protected against brute-force password guessing by implementing at least one of: • multi-factor authentication • 'throttling' the rate of attempts, so that the length of time the user must wait between attempts increases with each unsuccessful attempt – you shouldn't allow more than 10 guesses in 5 minutes • locking devices after no more than 10 unsuccessful attempts	To protect accounts in our organization from brute force password guessing, we use the following measures: 1. Multi-Factor Authentication: We require multi-factor authentication to guard initial access to all devices, applications, and services. This means that even if a password is compromised, an attacker cannot gain access without using biometrics or a mobile device. 2. Rate Limiting: For all internet-accessible services and systems we throttle login attempts from a single IP address, permitting no more than 10 login attempts in any 5-minute period. 3. Account Lockout Policy: For all internet-accessible services and systems, and wherever else possible, we configure an account lockout policy that locks the account for a user who enters the wrong password 10 times consecutively. 4. Strong Password Requirements: Our password policy requires the use of auto-generated strong passwords that are at least 12 characters and include a mix of uppercase and lowercase letters, numbers, and special characters. 5. Monitoring and Alerts: We continuously monitor for suspicious login activities, such as multiple failed login attempts, and use alerts to trigger prompt investigation of such incidents.	Compliant

A7.11 Password Quality Which technical controls are used to manage the quality of your passwords within your organisation? Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the section about Password-based authentication in the 'Cyber Essentials Requirements for IT Infrastructure' document. Cyber Essentials Requirements for IT Infrastructure v3.2 **CE Requirement**: Use technical controls to manage the quality of passwords. This will include one of the following: • using multi-factor authentication • a minimum password length of at least 12 characters, with no maximum length restrictions • a minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list.	Our organisational password policy is as follows: 1. Passwords of at least 12 characters in length, including a mixture of letters, cases, numbers, and symbols 2. Auto-generated by a password manager to avoid use of common passwords (see below) 3. Where the software / service enables it, multi-factor authentication to confirm user identity We use password managers to assist with password generation and usage, applying the following controls: 1. Master passwords for the password manager are created from 3 random words, capitalised in places and with numbers substituted for some letters. 2. Master passwords are committed to memory. 3. A biometric test is also required to access the password manager. Our GCloud and Google Workspace are configured to automatically block the use of common passwords by utilizing a deny list. This restricts users from setting passwords that are easily guessable or widely known to be compromised.	Compliant

A7.12 Password Creation Advice Please explain how you encourage people to use unique and strong passwords. You need to support those that have access to your organisational data and services by informing them of how they should pick a strong and unique password. Further information can be found in the Password-based authentication section, under the User Access Control section in the Cyber Essentials Requirements for IT Infrastructure document. Cyber Essentials Requirements for IT Infrastructure v3.2 **CE Requirement**: Support users to choose unique passwords for their work accounts by: • educating people about avoiding common passwords, such as a pet's name, common keyboard patterns or passwords they have used elsewhere. This could include teaching people to use the password generator feature built into some password managers • encouraging people to choose longer passwords by promoting the use of multiple words (a minimum of three) to create a password (such as the NCSC's guidance on using three random words) • providing usable secure storage for passwords (for example a password manager or secure locked cabinet) with clear information about how and when it can be used • not enforcing regular password expiry • not enforcing password complexity requirements	Our password policy insists that all passwords are: 1. At least 12 characters in length 2. A mixture of letters, cases, numbers, and symbols 3. Generated by a password manager to avoid accidental use of common passwords Note that master passwords for password managers are: 1. Created from 3 random words, capitalised in places and with numbers substituted for some letters 2. Committed to memory Multi-Factor Authentication is required to access software firewalls and password managers. These policies are supported by ongoing staff education about: 1. The risks associated with weak or reused passwords, showing how malicious entities might discover or break weak passwords. 2. The importance of password security and the benefits of using a password manager both to generate and to store passwords. 3. The simplicity of generated a strong but memorable password for the password manager itself. 4. The harm done to organisations whose security is breached, illustrating this with emotive examples such as the impact on the NHS of the WannaCry ransomware attack in May 2017.	Compliant

A7.13 Password Compromise Policy Do you have a process for when you believe the passwords or accounts have been compromised? You must have an established process that details how to change passwords promptly if you believe or suspect a password or account has been compromised. **CE Requirement:** You should make sure there is an established process in place to change passwords promptly if you know or suspect a password or account has been compromised. Further guidance : Compromised accounts	Yes Custom Fields: Applicant Notes: 1. Immediate Isolation: As soon as a potential password compromise is identified, we immediately isolate the affected accounts by temporarily suspending access to prevent further unauthorized use. 2. Incident Assessment: We conduct a preliminary assessment to understand the scope and impact of the compromise. This involves identifying the affected accounts, services, and users. 3. Notification and Communication: All relevant parties, including affected external service providers, are notified of the potential compromise. 4. Password Reset: We initiate a forced password reset for all affected accounts and any other accounts that may have been at risk. New passwords adhere to our password policy, which includes length requirements, complexity, and uniqueness. 5. Enhanced Authentication: For critical accounts, we may enforce any additional security measures that have become available, such as enabling multi-factor authentication (MFA) to add an extra layer of security. 6. Security Patch and Review: To mitigate the risk of further breaches, we apply any necessary security patches or updates to the systems involved. We also review security logs and conduct a comprehensive analysis to understand how the compromise occurred. 7. Updating Procedures: We review and update our cybersecurity procedures and training materials, as necessary, to incorporate lessons learned from the incident. 8. User Guidance: To help prevent future incidents, we reissue guidance to all staff on creating strong passwords and recognizing signs of potential compromises. 9. Extraordinary Audit: Following incident resolution, we conduct an extraordinary audit of all passwords and access controls to ensure continued compliance with our security policies.	Compliant

A7.14 Cloud Service MFA Do all of your cloud services have multi-factor authentication (MFA) available as part of the service? Where your systems and cloud services support multi-factor authentication (MFA), for example, a text message, a one-time access code, notification from an authentication app, then you must enable this for all users and administrators. For more information see the NCSC's guidance on MFA at Multi-factor authentication for your corporate online services Where a cloud service does not have its own MFA solution but can be configured to link to another cloud service to provide MFA, the link will need to be configured. A lot of cloud services use another cloud service to provide MFA. Examples of cloud services that can be linked to are Azure, MS365, Google Workspace. **CE Requirement**: Your organisation must implement MFA, where available – authentication to cloud services must always use MFA. Further guidance : Applying MFA to access cloud services Securing Your Cloud Services	Yes	Compliant
A7.16 Administrator MFA Has MFA been applied to **all** administrators of your cloud services? It is required that all administrator accounts on cloud service must apply multi-factor authentication in conjunction with a password of at least 8 characters. **CE Requirement**: Your organisation must implement MFA, where available – authentication to cloud services must always use MFA.	Yes	Compliant

A7.17 User MFA Has MFA been applied to **all** users of your cloud services? All users of your cloud services must use MFA in conjunction with a password of at least 8 characters. **CE Requirement**: Your organisation must implement MFA, where available – authentication to cloud services must always use MFA.	Yes	Compliant

A8.1 Malware Protection Are all of your desktop computers, laptops, tablets and mobile phones protected from malware by either: A - Having anti-malware software installed and/or B - Limiting installation of applications by application allow listing - for example, using an app store and a list of approved applications, using a Mobile Device Management (MDM) solution or C - None of the above, please describe Please select all the options that are in use in your organisation across all your devices. Most organisations that use smartphones and standard laptops will need to select both option A and B. • Option A - option for all in-scope devices running Windows or macOS including servers, desktop computers, laptop computers • Option B - option for all in-scope devices • Option C - none of the above, explanation notes will be required. **CE Requirement**: You must make sure that a malware protection mechanism is active on all devices in scope. For each device, you must use at least one of the options listed below. • Anti-malware software (option for in-scope devices running Windows or MacOS including servers, desktop computers, laptop computers) • Application allow listing (option for all in-scope devices). Only approved applications, restricted by code signing, are allowed to execute on devices.	0: A - anti-malware software, 1: B - limiting installation of applications by application allow listing from an approved app store	Compliant

A8.2 Anti-malware Updates If Option A has been selected: Where you have anti-malware software installed, is it set to update in line with the vendor's guidelines and prevent malware from running on detection? This is usually the default setting for anti-malware software. You can check these settings in the configuration screen for your anti-malware software. You can use any commonly used anti-malware product, whether free or paid-for as long as it can meet the requirements in this question. For the avoidance of doubt, Windows Defender is suitable for this purpose. **CE Requirement**: If you use anti-malware software to protect your device it must be configured to: • be updated in line with vendor recommendations • prevent malware from running • prevent the execution of malicious code	Yes	Compliant
A8.3 Scanning Web Pages If Option A has been selected: Where you have anti-malware software installed, is it set to scan web pages you visit and warn you about accessing malicious websites? Your anti-malware software or internet browser should be configured to prevent access to known malicious websites. On Windows 11, MS Defender SmartScreen can provide this functionality. **CE Requirement**: If you use anti-malware software to protect your device it must be configured to: • prevent connections to malicious websites over the internet.	Yes	Compliant

A8.4 Application Signing If Option B has been selected: Where you use an app-store or application signing, are users restricted from installing unsigned applications? Some operating systems which include Windows, Chromebooks, mobile phones and tablets restrict you from installing unsigned applications. Usually you have to "root" or "jailbreak" a device to allow unsigned applications. **CE Requirement**: Only approved applications, restricted by code signing, are allowed to execute on devices.	Yes	Compliant
A8.5 Approved Application List If Option B has been selected: Where you use an app-store or application signing, do you ensure that users only install applications that have been approved by your organisation and do you maintain this list of approved applications? You must create a list of approved applications and ensure users only install these applications on their devices. This includes employee-owned devices. You may use Mobile Device Management (MDM) software to meet this requirement but you are not required to use MDM software if you can meet the requirements using good policy, processes and training of staff. **CE Requirement:** • actively approve such applications before deploying them to devices • maintain a current list of approved applications, users must not be able to install any application that is unsigned or has an invalid signature	Yes Custom Fields: Applicant Notes: We use Google Workspaces built-in MDM functions	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