# Cyber Essentials Scheme

Report date: 30/3/2026
Applicant: Aseto,

Validated by: Antonis Koumantaris, Chief product officer & IT Systems Security Management

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 **0aec30e4-94fa-4ab8-86e2-6513fb33a8bf** and can be found here:

https://registry.blockmarktech.com/certificates/0aec30e4-94fa-4ab8-86e2-6513fb33a8bf/

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

## Applicant Answers

| | Applicant Answers | Assessor Score |
|---|---|---|
| Acceptance<br><br>Please read these terms and conditions carefully. Do you agree to these terms?<br><br>NOTE: if you do not agree to these terms, your answers will not be assessed or certified. | I accept | Compliant |
| A1.1 Organisation Name?<br><br>What is your organisation's name?<br><br>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.<br><br>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.<br><br>For example:<br><br>The Stationery Group, incorporating The Paper Mill and The Pen House<br>It is also possible to list on a certificate where organisations are trading as other names.<br><br>For example:<br><br>The Paper Mill trading as The Pen House. | GK Aseto Management LTD | Compliant |

| | | |
|---|---|---|
| A1.2 Organisation Type<br><br>What type of organisation are you?<br><br>"LTD" – Limited Company (Ltd or PLC)<br>"LLP" – Limited Liability Partnership (LLP)<br>"CIC" – Community Interest Company (CIC)<br>"COP" – Cooperative<br>"MTL" – Other Registered Mutual (Community Benefit Society, Credit Union, Building Society, Friendly Society)<br>"CHA" – Registered Charity<br>"GOV" – Government Agency or Public Body<br>"SOL" – Sole Trader<br>"PRT" – Other Partnership<br>"SOC" – Other Club/ Society<br>"OTH" – Other Organisation | LTD - Limited Company (Ltd or PLC) | Compliant |
| A1.3 Organisation Number<br><br>What is your organisation's registration number?<br><br>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).<br><br>There is a 20 character limit for your answer.<br>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".<br>If you are registered in a country that does not issue a company number, please enter a unique identifier like a DUNS number. | HE443550 | Compliant |
| A1.4 Organisation Address<br><br>What is your organisation's address?<br><br>Please provide the legal registered address for your organisation. | Rest of World<br><br>Custom Fields:<br>Address Line 1:<br>Eleftherias 30, Flat 201,Aradippou<br>Town/City:<br>Larnaca<br>Postcode:<br>7102<br>Country:<br>Cyprus | Compliant |

| | | |
|---|---|---|
| A1.5 Organisation Occupation<br><br>What is your main business?<br><br>Please summarise the main occupation of your organisation. | IT | Compliant |
| A1.6 Website Address<br><br>What is your website address?<br><br>Please provide your website address (if you have one). This can be a Facebook/LinkedIn page if you prefer. | www.aseto.ai | Compliant |
| A1.7 Renewal or First Time Application<br><br>Is this application a renewal of an existing certification or is it the first time you have applied for certification?<br><br>If you have previously achieved Cyber Essentials, please select "Renewal". If you have not previously achieved Cyber Essentials, please select "First Time Application". | First Time Application | Compliant |
| A1.8 Reasons for Certification<br><br>What are the two main reasons for applying for certification?<br><br>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 Commercial Contract<br><br>Custom Fields:<br>Secondary Reason:<br>Required for Government Contract | Compliant |
| A1.8.1 Commercial Contract Organisation<br><br>Who is the commercial contracting organisation?<br><br>Please provide the name of the contracting organisation. | N/A | Compliant |

| | | |
|---|---|---|
| A1.8.2 Government Contract Organisation<br><br>Who is the government contracting organisation and the contract number?<br><br>Please provide the contract number and the contracting organisation. | N/A | Compliant |
| A1.9 CE Requirements Document<br><br>Have you read the 'Cyber Essentials Requirements for IT Infrastructure' document?<br><br>Document is available on the NCSC Cyber Essentials website and should be read before completing this question set.<br><br>Cyber Essentials Requirements for IT Infrastructure v3.2 | Yes | Compliant |
| A1.10 Cyber Breach<br><br>Can IASME and their expert partners contact you if you experience a cyber breach?<br><br>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<br><br>Can IASME contact you for research purposes?<br><br>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<br><br>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.<br><br>Your whole organisation includes all divisions, people and devices which access your organisation's data and services.<br><br>About Scope<br><br>Subset Scoping Guidance | Yes | Compliant |
| A2.3 Geographical Location<br><br>Please describe the geographical locations of your business which are in the scope of this assessment.<br><br>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). | Larnaca, Cyprus (Head Office) | Compliant |

| | | |
|---|---|---|
| A2.4 End User Devices<br><br>Please list the quantities and operating systems for your laptops, desktops and virtual desktops within the scope of this assessment.<br><br>**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.**<br><br>**Devices that are connecting to cloud services must be included.**<br><br>**A scope that does not include end user devices is not acceptable.**<br><br>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.<br><br>For example, “We have 25 DELL laptops running Windows 10 Professional version 22H2 and 10 MacBook laptops running MacOS Ventura"".<br><br>Please note, the edition and feature version of your Windows operating systems are required.<br><br>This applies to both your corporate and user owned devices (BYOD).<br>You do not need to provide serial numbers, MAC addresses or further technical information.<br><br>**Extended Security Update schemes**<br><br>For any end-of-life operating system that has an extended security update program, you must maintain the required subscription.<br><br>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.<br><br>Further guidance:<br><br>Operating System Support<br><br>Guidance to BYOD | We have 6 laptops and 1 desktop running Windows 11 Pro version 25H2 | Compliant |

| | | |
|---|---|---|
| A2.4.1 Thin Client Devices<br><br>Please list the quantity of thin clients within the scope of this assessment. Please include make and operating systems.<br><br>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).<br><br>Thin clients are commonly used to connect to a Virtual Desktop Solution.<br><br>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.<br><br>Cyber Essentials Requirements for IT Infrastructure v3.2 | 0 thin clients in scope | Compliant |
| A2.5 Server Devices<br><br>Please list the quantity of servers, virtual servers, virtual server hosts (hypervisors) and Virtual Desktop Infrastructure (VDI) servers. You must include the operating system.<br><br>Please list the quantity of all servers within the scope of this assessment.<br><br>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 | 7 desktop computers running Ubuntu Server 22.04 LTS. | Compliant |

| | | |
|---|---|---|
| A2.6 Mobile Devices<br><br>Please list the quantities of tablets and mobile devices within the scope of this assessment.<br><br>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.<br><br>Devices that are connecting to cloud services must be included.<br><br>A scope that does not include end user devices is not acceptable.<br><br>Guidance to BYOD<br><br>Operating System Support | iPhone 13 Pro Max iOS iOS 26.4<br>iPhone 14 Pro Max iOS 26.4<br>iPhone 14 Pro iOS iOS 26.4<br>Samsung Galaxy Z Flip 7 Android 16 | Compliant |
| A2.7 Networks<br><br>Please provide a list of networks that will be in scope for this assessment.<br><br>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).<br><br>You do not need to provide IP addresses or other technical information. | Main Office Network Aradippou, Larnaca Used for company operations, development, servers, and administrative work. | Compliant |
| A2.7.1 Home or remote workers<br><br>How many staff are home or remote workers?<br><br>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.<br><br>For further guidance see the Home and remote working section in the Cyber Essentials Requirements for IT Infrastructure document.<br><br>Cyber Essentials Requirements for IT Infrastructure v3.2 | 0 (all work on-site) | Compliant |

| | | |
|---|---|---|
| A2.8 Network Equipment<br><br>Please provide a list of network equipment that will be in scope for this assessment (including firewalls and routers).<br><br>You must include make and model of each device listed.<br><br>You should include all equipment that controls the flow of data to and from the internet. This will be your routers and firewalls.<br><br>You do not need to include switches or wireless access points that do not contain a firewall or do not route internet traffic.<br><br>If you have home and/or remote workers they will be relying on software firewalls, please describe in the notes field.<br><br>You are not required to list any IP addresses, MAC addresses or serial numbers. | 1 x MikroTik RB5009 router/firewall (Main Office Network). | Compliant |
| A2.9 Cloud Services<br><br>Please list all of the cloud services that are in use by your organisation and provided by a third party.<br><br>**Please note that cloud services cannot be excluded from the scope of Cyber Essentials.**<br><br>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).<br><br>Definitions of the different types of cloud services are provided in the 'Cyber Essentials Requirements for IT Infrastructure' document.<br><br>Cyber Essentials Requirements for IT Infrastructure v3.2 | Google Workspace Suit, Microsoft Azure (API services to OpenAI) | Compliant |
| A2.10 Responsible Person<br><br>Please provide the name and role of the person who is responsible for managing your IT systems in the scope of this assessment.<br><br>This person must be a member of your organisation and cannot be a person employed by your outsourced IT provider. | Antonis Koumantaris<br><br>Custom Fields:<br>Responsible Person Role:<br>Chief product officer & IT Systems Security Management | Compliant |

| | | |
|---|---|---|
| A3.1 Head Office<br><br>Is your head office domiciled in the UK or Crown Dependencies and is your gross annual turnover less than £20m?<br><br>This question relates to the eligibility of your organisation for the included cyber insurance. | No | Compliant |
| A4.1 Boundary Firewall<br><br>Do you have firewalls at the boundaries between your organisation's internal networks, laptops, desktops, servers and the internet?<br><br>You must have firewalls in place between your office network and the internet.<br><br>**CE Requirement:** You must protect every device in scope with a correctly configured firewall (or network device with firewall functionality).<br><br>Further guidance:<br>Firewalls | Yes | Compliant |
| A4.1.1 Off Network Firewalls<br><br>Do you have software firewalls enabled on all of your computers, laptops and servers?<br><br>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.<br><br>Guidance on how to check your software firewall can be found here:<br><br>About Firewalls<br><br>**CE Requirement:** You must protect every device in scope with a correctly configured firewall (or network device with firewall functionality).<br><br>**CE Requirement:** Make sure you use a software firewall on devices which are used on untrusted networks, such as public wifi hotspots.<br><br>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<br><br>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?<br><br>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).<br><br>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.<br><br>**CE Requirement:** Change default administrative passwords to a strong and unique password – or disable remote administrative access entirely.<br><br>Further guidance:<br><br>About Routers | Yes | Compliant |

| | | |
|---|---|---|
| A4.2.1 Firewall Password Change Process<br><br>Please describe the process for changing your firewall password.<br><br>Home routers not supplied by your organisation are not included in this requirement.<br><br>You need to understand how the password on your firewall(s) is changed.<br><br>Please provide a brief description of how this is achieved. | The default administrator password on the MikroTik router/firewall is changed through a defined process during initial setup and maintained throughout the devices lifecycle.<br><br>Initial Setup Process:<br><br>The administrator connects to the router using the secure management interface . Upon first login, the default credentials are used only temporarily to gain access. Immediately after access is established, the administrator navigates to the user management section.<br>The default admin password is replaced with a strong, unique password that meets security requirements (minimum 12 characters, including a mix of uppercase, lowercase, numbers, and special characters).<br>The new password is saved, and the administrator logs out and logs back in to verify that the change has been successfully applied.<br><br>Ongoing Management Process:<br><br>Passwords are reviewed periodically in accordance with organizational security policies.<br>If required (e.g., policy schedule, suspected compromise, or staff changes), the administrator updates the password using the same secure management interface.<br>After each change, the administrator verifies successful implementation by re-authenticating with the new credentials.<br>Access logs and configuration settings are checked to ensure no unauthorized changes have occurred.<br><br>This process ensures that default credentials are not retained and that administrator access remains secure throughout the operational life of the device. | Compliant |

| | | |
|---|---|---|
| A4.3 Firewall Password Configuration<br><br>How is your firewall password configured?<br><br>Please select the options being used:<br><br>A. Multi-factor authentication, with a minimum password length 8 characters and no maximum length<br><br>B. Automatic blocking of common passwords, with a minimum password length 8 characters and no maximum length<br><br>C. A password minimum length of 12 characters and no maximum length<br><br>D. Passwordless system is being used as an alternative to user name and password, please describe<br><br>E. None of the above, please describe<br><br>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.<br><br>Cyber Essentials Requirements for IT Infrastructure v3.2<br><br>**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:<br><br>• multi-factor authentication<br>• an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach<br><br>Further guidance :<br><br>Bulletproof your passwords | 0: C. A password minimum length of 12 characters and no maximum length | Compliant |

| | | |
|---|---|---|
| A4.4 Firewall Password Issue<br><br>Do you change your firewall password when you know or suspect it has been compromised?<br><br>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.<br><br>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.<br><br>**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.<br><br>Further guidance:<br><br>Compromised Accounts | Yes | Compliant |
| A4.5 Firewall Management Process<br><br>Do you have a process to manage your firewall?<br><br>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 | Compliant |

| | | |
|---|---|---|
| A4.6 Firewall Review Process<br><br>Have you reviewed your firewall rules in the last 12 months?<br><br>Please describe your review process.<br><br>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?).<br><br>**CE Requirement:** Remove or disable inbound firewall rules quickly when they are no longer needed. | Firewall rules on the MikroTik router/firewall are managed through a formal review and verification process.<br><br>Review Process:<br><br>Firewall rules are reviewed on a quarterly basis (every 3 months) by the designated system administrator/network administrator.<br>During each review, the administrator:<br>Examines all existing firewall rules and open ports.<br>Identifies and removes any unused, obsolete, or unnecessary rules.<br>Confirms that only required services and ports remain enabled in line with business and security requirements.<br>Any proposed changes are documented before implementation.<br><br>Implementation and Verification:<br><br>Approved changes are applied through the secure management interface.<br>After implementation, a second responsible party (e.g., IT manager or senior administrator) performs a verification check to ensure:<br>The changes have been correctly applied.<br>No unintended services or ports remain open.<br>Firewall logs and rule configurations are reviewed to confirm expected behavior.<br>All changes and verification steps are recorded for audit purposes.<br><br>This structured process ensures firewall configurations remain secure, up to date, and compliant throughout the devices lifecycle. | Compliant |
| A4.7 Firewall Inbound Connections<br><br>Is your firewall configured to allow unauthenticated inbound connections?<br><br>By default, most firewalls block all services inside the network from being accessed from the internet, but you need to check your firewall settings.<br><br>**CE Requirement:** Block unauthenticated inbound connections by default. | No | Compliant |

| | | |
|---|---|---|
| A4.8 Allowed Connections<br><br>Please describe how you approve and document your allowed inbound connections.<br><br>The business case should be documented and recorded. A business case must be signed off at board level and associated risks reviewed regularly.<br><br>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.<br><br>**CE Requirement:** Ensure inbound firewall rules are approved and documented by an authorised person, and include the business need in the documentation. | Inbound connections are only allowed when there is a clear business need. Requests are approved by the system administrator, documented internally, and the required port is opened on the firewall. Rules are reviewed regularly and removed when no longer needed. | Compliant |

| | | |
|---|---|---|
| A4.9 Firewall Remote Configuration<br><br>Are your boundary firewalls configured to allow access to their configuration settings over the internet?<br><br>Sometimes organisations configure their firewall to allow other people (such as an IT support company) to change the settings via the internet.<br><br>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.<br><br>**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:<br><br>• multi-factor authentication<br>• an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach<br><br>Guidance on VPNs | No | Compliant |
| A5.1 Remove Unused Software<br><br>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?<br>Describe how you achieve this.<br><br>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.<br><br>To view installed applications:<br><br>Windows: Right-click on Start > Apps and Features<br><br>macOS: Open Finder > Applications<br><br>Linux: Open your software package manager (apt, rpm, yum) | Unnecessary software, services, and applications are removed and controlled through a defined manual management and review process applied to all devices, including laptops, desktops, servers, cloud systems, and mobile devices.<br><br>Initial Setup Process:<br><br>All devices are configured using a standard build procedure that defines approved operating systems, applications, and services.<br>During setup, the system administrator:<br>Reviews all pre-installed software and services.<br>Removes any non-essential or unauthorized applications using built-in operating system tools (e.g., Windows Add/Remove Programs, Linux package managers, macOS system settings).<br>For mobile devices, only approved applications are installed, and unnecessary default applications are removed or disabled where possible. | Compliant<br><br>Assessor Notes:<br>Needs some more detail on how this is achieved for your devices, are they managed centrally with an RMM solution or done on a per-machine basis, etc? Also needs to include mobile devices, as you have stated previously. |

| | | |
|---|---|---|
| **CE Requirement:** You must regularly remove or disable unnecessary software (including applications, system utilities and network services).<br><br>Further guidance : Removing unnecessary software | Ongoing Management Process:<br><br>Devices are managed on a per-machine basis by the system administrator.<br>An approved software list (baseline) is maintained and used as a reference for all systems.<br>The administrator periodically accesses each system to:<br>Review installed programs and running services.<br>Compare them against the approved baseline.<br>Remove any unauthorized or unused software.<br><br>Review Timeframe:<br><br>Software and services are reviewed on a quarterly basis (every 3 months), and additionally:<br>When a device is reassigned to another user.<br>After major system updates or changes.<br><br>Verification and Oversight:<br><br>After any removal or change:<br>The system administrator verifies the system by re-checking installed programs and services.<br>A second party (e.g., IT manager or senior administrator) performs periodic spot checks (e.g., quarterly sample reviews) to confirm:<br>Compliance with the approved software baseline.<br>That unauthorized applications have been removed.<br>Findings and actions are documented for audit purposes.<br><br>This process ensures that only required software and services are present on all systems, including mobile devices, without reliance on centralized management tools, while maintaining compliance through documented procedures and independent verification. | |

| | | |
|---|---|---|
| A5.2 Remove Unrequired User Accounts<br><br>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?<br><br>You must remove or disable any user accounts that are not needed in day-to-day use on all devices and cloud services.<br><br>To view user accounts:<br><br>Windows: Right-click on Start > Computer Management > Users<br><br>macOS: System Settings > Users and Groups<br><br>Linux: "cat/etc/passwd"<br><br>**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<br><br>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?<br><br>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".<br><br>**CE Requirement:** You must regularly change any default or guessable account passwords.<br><br>Use technical controls to manage the quality of passwords. This will include one of the following:<br><br>• using multi-factor authentication<br>• a minimum password length of at least 12 characters, with no maximum length restrictions<br>• 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<br><br>Do you run or host external services that provide access to data (that shouldn't be made public) to users across the internet?<br><br>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.<br><br>**CE Requirement:** Ensure users are authenticated before allowing them access to organisational data or services. | Yes | Compliant |

| | | |
|---|---|---|
| A5.5 External services Authentication<br><br>If yes to question A5.4, which authentication option do you use?<br><br>A. Multi-factor authentication, with a minimum password length of 8 characters and no maximum length<br><br>B. Automatic blocking of common passwords, with a minimum password length of 8 characters and no maximum length<br><br>C. A minimum password length of 12 characters and no maximum length<br><br>D. Passwordless, please describe<br><br>E. None of the above, please describe<br><br>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.<br><br>Cyber Essentials Requirements for IT Infrastructure v3.2<br><br>**CE Requirement**: Use technical controls to manage the quality of passwords. This will include one of the following:<br><br>• using multi-factor authentication<br>• a minimum password length of at least 12 characters, with no maximum length restrictions<br>• a minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list | 0: C. A minimum password length of 12 characters and no maximum length | Compliant |

| | | |
|---|---|---|
| A5.6 External services password change process<br><br>Describe the process in place for changing passwords on your external services when you believe they have been compromised.<br><br>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.<br><br>**CE Requirement**: You should also make sure there is an established process in place to change passwords promptly if you know or suspect a password or account has been compromised. | If a password compromise is suspected, the affected account password is immediately reset by the system administrator, sessions are revoked, logs are reviewed, and access credentials are replaced with a new strong password. | Compliant |

| | | |
|---|---|---|
| A5.7 External services brute-force protection<br><br>When not using multi-factor authentication, which option are you using to protect your external service from brute force attacks?<br><br>A. Throttling the rate of attempts<br><br>B. Locking accounts after 10 unsuccessful attempts<br><br>C. None of the above, please describe<br><br>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.<br><br>**CE Requirement:** You must protect your chosen authentication method (which can be biometric authentication, password or PIN) against brute-force attacks. When it's possible to configure, you should apply one of the following:<br><br>• '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<br>• locking devices after more than 10 unsuccessful attempts<br>• When the vendor doesn't allow you to configure the above, use the vendor's default setting. | 0: A. Throttling the rate of attempts | Compliant |

| | | |
|---|---|---|
| A5.8 Auto-run Disabled<br><br>Have you disabled any feature which allows automatic file execution of downloaded or imported files without user authorisation?<br><br>This is a setting on your device which automatically runs software on external media or downloaded from the internet.<br><br>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.<br><br>**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<br><br>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?<br><br>Device locking mechanisms such as biometric, password or PIN, need to be enabled to prevent unauthorised access to devices accessing organisational data or services.<br><br>**CE Requirement:** Ensure appropriate device locking controls for users that are physically present. | Yes | Compliant |

| | | |
|---|---|---|
| A5.10 Device Unlocking Method<br><br>Which method do you use to unlock the devices?<br><br>Please refer to Device Unlocking Credentials paragraph found under Secure Configuration in the Cyber Essentials Requirements for IT Infrastructure document for further information.<br><br>Cyber Essentials Requirements for IT Infrastructure v3.2<br><br>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.<br><br>**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.<br><br>You must protect your chosen authentication method against brute-force attacks.<br><br>When it's possible to configure, you should apply one of the following:<br><br>• '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<br>• locking devices after more than 10 unsuccessful attempts<br>• When the vendor doesn't allow you to configure the above, use the vendor's default setting. | User devices are protected using secure unlocking methods appropriate to the device type, with enforced controls to prevent brute-force attacks.<br><br>Mobile Devices (Phones):<br><br>Access is controlled using biometric authentication (e.g., fingerprint or facial recognition) combined with a strong passcode/password as a fallback.<br>Devices are configured so that authentication attempts are protected by operating system security controls, including:<br>Locking of the device after 10 consecutive failed authentication attempts, or<br>Throttling of login attempts to no more than 10 attempts within a 5-minute period, depending on device capabilities and vendor defaults.<br><br>Laptops and Desktops:<br><br>Access is controlled using strong passwords in line with organisational policy (minimum length, complexity, and uniqueness requirements).<br>Systems are configured to protect against brute-force attacks through:<br>Account lockout after 10 failed login attempts, and/or<br>Throttling of login attempts to no more than 10 attempts within a 5-minute period, enforced via operating system security policies (e.g., Windows Local/Group Policy or Linux PAM configuration).<br><br>Verification and Enforcement:<br><br>These settings are applied during device setup and verified by the system administrator.<br>Authentication and lockout configurations are reviewed on a quarterly basis (every 3 months).<br>A second party (e.g., IT manager or senior administrator) performs periodic checks to confirm that lockout/throttling policies are correctly enforced across devices.<br><br>This ensures that all user devices are protected against unauthorized access and brute-force attacks using clearly defined and enforced controls. | Compliant<br><br>Assessor Notes:<br>With the devices you have mentioned i would be expecting to see you explicitly mention either Throttling of attempts with no more than 10 tries in 5 min or locking of devices after 10 attempts. |

| | | |
|---|---|---|
| A6.1 Supported Operating System<br><br>Are all operating systems on your devices supported by a vendor that produces regular security updates and vulnerability fixes?<br><br>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.<br><br>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<br><br>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.<br><br>**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.<br><br>Vulnerability fixes include patches, updates, registry fixes, configuration changes, scripts or any other mechanism approved by the vendor to fix a known vulnerability.<br><br>**Extended Security Update schemes**<br><br>For any end-of-life operating system that has an extended security update program, you must maintain the required subscription.<br><br>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.<br><br>Further guidance:<br><br>Operating System Support<br><br>Navigating the pitfalls of legacy software | Yes | Compliant |

| | | |
|---|---|---|
| A6.2 Supported software<br><br>Is all the software on your devices supported by a supplier that produces regular vulnerability fixes for any security problems?<br><br>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.<br><br>**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<br><br>Please list your internet browser(s). The version is required.<br><br>Please list all internet browsers installed on your devices, so that the Assessor can understand your setup and verify that they are in support.<br><br>For example: Chrome Version 124, Safari Version 15.<br><br>**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. | Desktop Browsers:<br>Google Chrome<br>Version: 146.0.7680.72 (Stable channel March 2026 release)<br>Microsoft Edge<br>Version: 146.0.3856.59 (Stable channel March 2026)<br><br>Mobile Device Browsers:<br><br>iOS Devices (iPhone/iPad):<br>Safari (iOS)<br>Version: 26.4 (aligned with iOS/iPadOS 26.3)<br><br>Android Devices (including Samsung devices):<br>Google Chrome (Android)<br>Version: 146.0.76380.111 (Stable release, March 2026)<br>Samsung Internet Browser (default on Samsung devices)<br>Version: 29.0.4.46 (current stable version)<br><br>Management and Verification Process<br>Browsers are installed during system setup in line with an approved software baseline.<br>All browsers are configured to update automatically via:<br>Built-in browser update services (desktop)<br>Apple App Store (iOS devices)<br>Google Play Store (Android devices)<br>Browser versions are reviewed on a quarterly basis (every 3 months) by the system administrator, including:<br>Desktop devices<br>iOS devices<br>Android/Samsung devices<br>A second party (e.g., IT manager or senior administrator) performs periodic checks to confirm:<br>All browsers are running supported versions<br>Automatic updates are enabled and functioning correctly<br>Any browser found to be outdated or unsupported is updated immediately or removed.<br><br>Compliance Statement<br><br>All internet browsers in use are:<br><br>Fully supported by the vendor<br>Kept up to date with current stable versions<br>Configured for automatic updates | Compliant<br><br>Assessor Notes:<br>You mentioned an Android device in your CE earlier; however, within this answer, you only mention Apple devices and App stores. Can you include your Android device as well?<br>Also, for versions i do need version numbers to be included, even when aligned with OS versions. Please list full version numbers when required. Your Samsung device will also have its default browser installed, most likely, which will need to be included. |

| | | |
|---|---|---|
| A6.2.2 Malware Protection<br><br>Please list your malware protection software<br>The version is required.<br><br>Please list all malware protection and versions you use so that the Assessor can understand your setup and verify that they are in support.<br><br>For example: Sophos Endpoint Protection V10, Microsoft Defender, Bitdefender Internet Security 2023.<br><br>**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. | Malware protection is implemented using built-in, supported security software across all devices and is configured for real-time protection and automatic updates.<br><br>Malware Protection Software in Use:<br><br>Microsoft Defender Antivirus (Windows devices)<br>Platform Version: 4.18.26010.5<br>Engine Version: 1.1.26010.1<br>Security Intelligence Version: 1.445.6.0 (example current baseline; definitions update multiple times daily)<br>Apple Built-in Malware Protection (macOS / iOS devices XProtect, Gatekeeper, MRT)<br>Version: Integrated within the operating system (e.g., current supported macOS / iOS versions with latest security updates applied)<br>Updates are delivered automatically via OS security updates.<br><br>Configuration and Management:<br><br>Microsoft Defender Antivirus is enabled by default on all Windows devices and configured with:<br>Real-time protection<br>Cloud-delivered protection<br>Automatic submission of samples<br>Updates for platform, engine, and security intelligence are delivered automatically via Windows Update, with security intelligence updates released multiple times per day.<br>Apple devices rely on built-in protections (XProtect, Gatekeeper), which are automatically updated through system updates.<br><br>Verification and Review Process:<br><br>Malware protection status and exact version numbers are checked on a quarterly basis (every 3 months) by the system administrator, including:<br>Verification of Defender platform, engine, and security intelligence versions on Windows devices<br>Confirmation that Apple devices are running supported OS versions with current security updates<br>After each review, the administrator confirms:<br>Real-time protection is enabled<br>Definitions are up to date and actively updating<br>A second party (e.g., IT manager or senior administrator) performs periodic spot checks to verify:<br>Version numbers match current supported releases<br>Updates are being successfully applied<br>Any device found to be out of date is | Compliant<br><br>Assessor Notes:<br>Need to know the exact version numbers of the malware protection in use, stating the latest version is not a satisfactory answer for Cyber Essentials. |

| | | |
|---|---|---|
| | updated immediately and revalidated. | |
| A6.2.3 Email Applications<br><br>Please list your email applications installed on end user devices and server. The version is required.<br><br>Please list all email applications and versions you use so that the Assessor can understand your setup and verify that they are in support.<br><br>For example: MS Exchange 2016, Outlook 2019.<br><br>**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. | Email services are provided using cloud-hosted solutions and are accessed securely via both web browsers and mobile applications.<br><br>Email Services in Use:<br><br>Gmail (Google Workspace Web Application)<br>Managed by Google<br>Version: Not applicable (software is vendor-managed and continuously updated as a SaaS service)<br>Access Method: Web browsers (e.g., Google Chrome, Microsoft Edge)<br>Gmail Mobile Application (iOS / Android devices)<br>Version: 6.0.240303 (iOS/Android March 2026 release baseline)<br>Updates: Delivered via Apple App Store / Google Play Store automatic updates<br><br>Device Coverage:<br><br>Desktops and Laptops:<br>Email is accessed exclusively via web browsers.<br>No locally installed email clients (e.g., Microsoft Outlook) or on-premise mail servers are used.<br>Mobile Devices (Phones):<br>Email is accessed via the official Gmail mobile application.<br>Devices are configured to require secure authentication (passcode/biometric) before access to email.<br>Application updates are enabled automatically via the device app store.<br><br>Configuration and Management Process:<br><br>Email services are provisioned through Google Workspace and managed centrally via the admin console.<br>Only authorised user accounts are granted access to email services.<br>Mobile devices accessing email are configured in line with organisational security requirements (e.g., screen lock, up-to-date OS).<br><br>Verification and Review Process:<br><br>Email access methods and application versions are reviewed on a quarterly basis (every 3 months) by the system administrator, including:<br>Confirming browsers are up to date on desktops/laptops<br>Verifying the Gmail mobile app version on a sample of devices<br>A second party (e.g., IT manager or senior administrator) performs periodic checks to ensure:<br>Only approved methods of email access | Compliant<br><br>Assessor Notes:<br>What about your mobile devices? If you have emails on the phones, they will be included in this question. |

| | | |
|---|---|---|
| | are in use<br>Applications are up to date and supported<br>Any outdated applications or unsupported access methods are updated or removed immediately. | |
| A6.2.4 Office Applications<br><br>Please list all office applications that are used to create organisational data.<br>The version is required.<br><br>Please list all office applications and versions you use so that the Assessor can understand your setup and verify that they are in support.<br><br>For example: MS 365, Libre Office, Google Workspace, Office 2016.<br><br>**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. | Office Applications in Use<br>Google Docs (Web Application accessed via web browser)<br>Google Sheets (Web Application accessed via web browser)<br>Google Slides (Web Application accessed via web browser)<br>Gmail (Web Application accessed via web browser for communication and data exchange)<br><br>All of the above applications are part of Google Workspace and are used exclusively in their web-based versions, with no locally installed office software in use.<br><br>These applications form part of the Google Workspace suite, which is a cloud-based productivity platform accessed via web browsers and mobile applications.<br><br>Google Workspace Applications (Docs, Sheets, Slides, Gmail Web Versions)<br>Version: Not applicable (Software-as-a-Service)<br><br>These applications do not have fixed version numbers because they are delivered as SaaS and are continuously updated by the vendor.<br><br>Updates, patches, and security fixes are applied automatically by Google<br>Users always access the current supported version via the browser<br><br>Additionally, Google confirms that Workspace tools are always up to date and accessible from any device. | Compliant<br><br>Assessor Notes:<br>If you are using the web version, please state explicitly in the answer. |

| | | |
|---|---|---|
| A6.3 Software Licensing<br><br>Are any of the in-scope software or cloud services unlicensed or unsupported?<br><br>All software must be licensed. It is acceptable to use free and open-source software as long as you comply with any licensing requirements.<br><br>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.<br><br>**CE Requirement:** All software on in-scope devices must be licensed and supported. | No | Compliant |

| | | |
|---|---|---|
| A6.4 Security Updates - Operating System<br><br>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?<br><br>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.<br><br>This requirement includes the firmware on your firewalls and routers.<br><br>**CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where:<br><br>• The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk'<br>• The update addresses vulnerabilities with a CVSSv3 base score of 7 or above<br>• There are no details of the level of vulnerabilities the update fixes provided by the vendor<br><br>Please note: For optimum security we strongly recommend (but it's not mandatory) that all released updates are applied within 14 days of release.<br><br>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<br><br>Are all updates applied for operating systems by enabling auto updates?<br><br>Most devices have the option to enable auto updates. This must be enabled on any device where possible.<br><br>**CE Requirement**: All software on in-scope devices must have automatic updates enabled where possible. | Yes | Compliant |

| | | |
|---|---|---|
| A6.4.2 Manual Updates - Operating System<br><br>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?<br><br>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.<br><br>Please describe how any updates are applied when auto updates are not configured.<br><br>If you only use auto updates, please confirm this in the notes field for this question.<br><br>**CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where:<br><br>• The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk'<br>• The update addresses vulnerabilities with a CVSSv3 base score of 7 or above<br>• There are no details of the level of vulnerabilities the update fixes provided by the vendor | Automatic updates are enabled on all operating systems and network devices wherever supported. Systems are configured to automatically download and install security updates to ensure they remain protected against known vulnerabilities.<br><br>Patch Management Process:<br><br>All devices are configured to receive updates automatically via vendor update services (e.g., Windows Update, Apple Software Update).<br>High and critical security updates are applied within 14 days of release, in line with Cyber Essentials requirements.<br>Where automatic updates are not immediately applied, the system administrator manually checks for and installs updates to ensure compliance with the 14-day requirement.<br><br>Verification and Monitoring:<br><br>The system administrator performs regular checks (at least weekly) to confirm that updates are being successfully applied.<br>A monthly review is conducted to verify that all devices have received relevant security updates within the required timeframe.<br>A second party (e.g., IT manager or senior administrator) performs periodic checks to confirm:<br>High and critical updates have been installed within 14 days<br>No devices are missing important security patches<br><br>Exception Handling:<br><br>If an update cannot be applied within 14 days (e.g., due to compatibility issues), this is:<br>Documented<br>Risk assessed<br>Remediated as soon as possible<br><br>This process ensures that all systems remain up to date and that high and critical vulnerabilities are addressed within the required timeframe. | Compliant<br><br>Assessor Notes:<br>Please confirm high and critical updates are installed within 14 days of release. |

| | | |
|---|---|---|
| A6.5 Security Updates - Applications<br><br>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?<br><br>You must install any such updates and vulnerability fixes within 14 days in all circumstances.<br><br>If you cannot achieve this requirement at all times, you will not achieve compliance to this question.<br><br>You are not required to install feature updates or optional updates in order to meet this requirement, just high-risk or critical security updates.<br><br>**CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where:<br><br>• The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk'<br>• The update addresses vulnerabilities with a CVSSv3 base score of 7 or above<br>• There are no details of the level of vulnerabilities the update fixes provided by the vendor | Yes | Compliant |
| A6.5.1 Auto-updates- Applications<br><br>Are all updates applied on your applications by enabling auto updates?<br><br>Most devices have the option to enable auto updates. Auto updates should be enabled where possible.<br><br>**CE Requirement:** All software on in-scope devices must have automatic updates enabled where possible. | Yes | Compliant |

| | | |
|---|---|---|
| A6.5.2 Manual Updates - Applications<br><br>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?<br><br>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.<br><br>Please describe how any updates and vulnerability fixes are applied when auto updates are not configured.<br><br>If you only use auto updates, please confirm this in the notes field for this question.<br><br>**CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where:<br><br>• The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk'<br>• The update addresses vulnerabilities with a CVSSv3 base score of 7 or above<br>• There are no details of the level of vulnerabilities the update fixes provided by the vendor | Most of our systems and applications are set to update automatically.<br><br>For anything that doesnt support auto-updates, we handle updates manually. We use OpenCVE to keep track of newly disclosed vulnerabilities and monitor anything that might affect our systems.<br><br>When a high-risk or critical issue is identified, we review it and apply the relevant updates as soon as possible, and always within 14 days. Updates are planned to minimise disruption, and we keep a simple record of what was updated and when. | Compliant |
| A6.6 Unsupported Software Removal<br><br>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?<br><br>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.<br><br>**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<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>Where no unsupported software is used across your whole organisation, please declare this here.<br><br>**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.<br><br>Further guidance: Subset Scoping Guidance | No unsupported software is used within the organisation.<br><br>All software in use is actively supported by the vendor and kept up to date through automatic updates or regular patching processes. Where software approaches end-of-life, it is reviewed and either upgraded or removed to ensure it does not become unsupported. | Compliant |
| A7.1 User Account Creation<br><br>Are your users only provided with user accounts after a process has been followed to approve their creation? Describe the process.<br><br>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.<br><br>**CE Requirement:** Your organisation must have in place a process to create and approve user accounts. | User accounts are created only after approval from management. The system administrator creates the account with the appropriate permissions after receiving approval from a director or authorised manager. | Compliant |

| | | |
|---|---|---|
| A7.2 Unique Credentials<br><br>Are all your user and administrative accounts accessed by entering unique credentials?<br><br>You must ensure that no devices, applications or cloud services can be accessed without entering unique access credentials.<br><br>Accounts must not be shared.<br><br>**CE Requirement:** Authenticate users with unique credentials before granting access to applications or devices. | Yes | Compliant |
| A7.3 Leaver Accounts<br><br>How do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation?<br><br>When an individual leaves your organisation, you need to stop them accessing any of your systems.<br><br>**CE Requirement:** Remove or disable user accounts when no longer required. | When a staff member leaves the organisation, their access is removed as part of the offboarding process.<br>The system administrator immediately disables or deletes their accounts and removes access to all systems and services. | Compliant |
| A7.4 User Privileges<br><br>Do you ensure that staff only have the access privileges that they need to do their current job? How do you do this?<br><br>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.<br><br>For Cyber Essentials we require that the principle of least privilege be applied.<br><br>**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. | Yes. Access permissions are assigned based on job role using the principle of least privilege. The system administrator grants only the permissions required for the employees duties and reviews access when roles change. | Compliant |

| | | |
|---|---|---|
| A7.5 Administrator Approval<br><br>Do you have a formal process for giving someone access to systems at an “administrator” level and can you describe this process?<br><br>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.<br><br>**CE Requirement:** Your organisation must have in place a process to create and approve user accounts. | Administrator access is granted only after approval from company management. The system administrator creates the administrator account only when required for operational tasks and records the approval internally. | Compliant |
| A7.6 Use of Administrator Accounts<br><br>How does your organisation make sure that separate accounts are used to carry out administrative tasks (such as installing software or making configuration changes)?<br><br>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.<br><br>Cloud service administration must be carried out using separate accounts.<br><br>Further guidance :<br><br>User Access - Just Enough or Just In Time<br><br>**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). | Administrative tasks are performed using separate administrator accounts that are different from standard user accounts used for daily work. | Compliant |

| | | |
|---|---|---|
| A7.7 Managing Administrator Account Usage<br><br>How does your organisation prevent administrator accounts from being used to carry out everyday tasks like browsing the web or accessing email?<br><br>This question relates to the activities carried out when an administrator account is in use.<br><br>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.<br><br>**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). | Administrator accounts are restricted to administrative tasks only. Staff use standard user accounts for email, browsing and normal work activities. | Compliant |
| A7.8 Administrator Account Tracking<br><br>Do you formally track which users have administrator accounts in your organisation?<br><br>You must track all people that have been granted administrator accounts.<br><br>**CE Requirement:** Your organisation must have in place a process to create and approve user accounts. | Yes | Compliant |
| A7.9 Administrator Access Review<br><br>Do you review who should have administrative access on a regular basis?<br><br>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.<br><br>**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<br><br>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?<br><br>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.<br><br>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.<br><br>Cyber Essentials Requirements for IT Infrastructure v3.2<br><br>**CE Requirement**: Passwords are protected against brute-force password guessing by implementing at least one of:<br><br>• multi-factor authentication<br>• '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<br>• locking devices after no more than 10 unsuccessful attempts | Systems are protected against brute-force attacks through enforced account lockout and login throttling mechanisms.<br><br>Brute-Force Protection Controls:<br><br>User accounts and devices are configured to lock after 10 consecutive failed login attempts, in line with Cyber Essentials requirements.<br>In addition, where supported by the operating system, login attempts are throttled to no more than 10 attempts within a 5-minute period.<br>These controls are enforced through built-in operating system security settings (e.g., Windows account lockout policies, mobile device security settings).<br><br>Implementation and Verification:<br><br>These settings are applied during system setup by the system administrator.<br>Configurations are reviewed on a quarterly basis (every 3 months) to ensure compliance.<br>A second party (e.g., IT manager or senior administrator) performs periodic checks to confirm that:<br>Account lockout is set to trigger after 10 failed attempts<br>Throttling controls are correctly enforced where applicable<br><br>This ensures that systems are effectively protected against brute-force attacks in accordance with Cyber Essentials requirements. | Compliant<br><br>Assessor Notes:<br>Please be specific to one of the CE requirements listed in the question, be it MFA, throttling with no more than 10 guesses in 5 minutes or locking devices after 10 attempts. |

| | | |
|---|---|---|
| A7.11 Password Quality<br><br>Which technical controls are used to manage the quality of your passwords within your organisation?<br><br>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.<br><br>Cyber Essentials Requirements for IT Infrastructure v3.2<br><br>**CE Requirement**: Use technical controls to manage the quality of passwords. This will include one of the following:<br><br>• using multi-factor authentication<br>• a minimum password length of at least 12 characters, with no maximum length restrictions<br>• 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. | Passwords must be at least 12 characters long with no maximum length restrictions. | Compliant |

| | | |
|---|---|---|
| A7.12 Password Creation Advice<br><br>Please explain how you encourage people to use unique and strong passwords.<br><br>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.<br><br>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.<br><br>Cyber Essentials Requirements for IT Infrastructure v3.2<br><br>**CE Requirement**: Support users to choose unique passwords for their work accounts by:<br><br>• 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<br>• 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)<br>• 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<br>• not enforcing regular password expiry<br>• not enforcing password complexity requirements | We support staff in creating strong and unique passwords through simple guidance and good practices.<br><br>Users are encouraged to:<br><br>Use longer passwords made up of multiple random words (e.g. three or more words)<br>Avoid common or easily guessed passwords (such as names, patterns, or reused passwords)<br>Use a password manager (where appropriate) to generate and securely store unique passwords for each account<br><br>We provide guidance during onboarding and remind users of good password practices when needed.<br><br>We do not enforce regular password expiry or overly complex rules, in line with current best practice, but instead focus on making passwords longer, unique, and easier to manage securely. | Compliant |

| | | |
|---|---|---|
| A7.13 Password Compromise Policy<br><br>Do you have a process for when you believe the passwords or accounts have been compromised?<br><br>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.<br><br>**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.<br><br>Further guidance : Compromised accounts | Yes | Compliant |
| A7.14 Cloud Service MFA<br><br>Do all of your cloud services have multi-factor authentication (MFA) available as part of the service?<br><br>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<br><br>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.<br><br>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.<br><br>**CE Requirement**: Your organisation must implement MFA, where available – authentication to cloud services must always use MFA.<br><br>Further guidance :<br><br>Applying MFA to access cloud services<br><br>Securing Your Cloud Services | Yes | Compliant |

| | | |
|---|---|---|
| A7.16 Administrator MFA<br><br>Has MFA been applied to **all** administrators of your cloud services?<br><br>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.<br><br>**CE Requirement**: Your organisation must implement MFA, where available – authentication to cloud services must always use MFA. | Yes | Compliant |
| A7.17 User MFA<br><br>Has MFA been applied to **all** users of your cloud services?<br><br>All users of your cloud services must use MFA in conjunction with a password of at least 8 characters.<br><br>**CE Requirement**: Your organisation must implement MFA, where available – authentication to cloud services must always use MFA. | Yes | Compliant |

| | | |
|---|---|---|
| A8.1 Malware Protection<br><br>Are all of your desktop computers, laptops, tablets and mobile phones protected from malware by either:<br><br>A - Having anti-malware software installed<br><br>and/or<br><br>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<br><br>or<br><br>C - None of the above, please describe<br><br>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.<br><br>• Option A - option for all in-scope devices running Windows or macOS including servers, desktop computers, laptop computers<br>• Option B - option for all in-scope devices<br>• Option C - none of the above, explanation notes will be required.<br><br>**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.<br><br>• Anti-malware software (option for in-scope devices running Windows or MacOS including servers, desktop computers, laptop computers)<br>• 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 | Compliant |

| | | |
|---|---|---|
| A8.2 Anti-malware Updates<br><br>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?<br><br>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.<br><br>**CE Requirement**: If you use anti-malware software to protect your device it must be configured to:<br><br>• be updated in line with vendor recommendations<br>• prevent malware from running<br>• prevent the execution of malicious code | Yes | Compliant |
| A8.3 Scanning Web Pages<br><br>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?<br><br>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.<br><br>**CE Requirement**: If you use anti-malware software to protect your device it must be configured to:<br><br>• prevent connections to malicious websites over the internet. | Yes | Compliant |
| All Answers Approved<br><br>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 |