Cyber Essentials Plus Assessment Report

Assessment of: Headhunter Systems T/A Gravyty

Assessed by (Certification Body): Commissum Associates Limited

Assessed By (Assessor Name): Jonny Lie

Assessed By (Lead Assessor name): Jonny Lie

Date of assessment visit: 27 to 28 November 2023

Date of Report: 29/11/2023

Cyber Essentials Plus certification can only be issued by a licensed Certification Body.

You can confirm the authenticity of this report by contacting IASME Consortium

+44 (0)3300 882752

1. About this report

Cyber Essentials Plus is the audited version of the Cyber Essentials information security standard. Cyber Essentials requires organisations to have a number of technical and procedural controls in place to improve their information security in order to mitigate common internet-borne cyber attacks. Cyber Essentials Plus is a series of tests that provide a further level of assurance that these technical controls have been successfully implemented within an organisation.

This report is a record of the Cyber Essentials Plus audit of Headhunter Systems T/A Gravyty against the Cyber Essentials standard that has been carried out by Jonny Lie of the Certifying Body Commissum Associates Limited.

Cyber Essentials provides assurance that a number of key information security controls are in place within an organisation. For further assurance, the IASME information security standard provides a broader set of controls that enable good information security governance across an organisation.

1.1 Summary of findings

Gravyty shown a good security implementation and passed the Cyber Essentials Plus assessment. No critical or high risk issues were found on the external perimeter, principle of least privilege was found to be implemented properly and anti-malware software was keep up-to-date as well. All accounts were revolved around Google where authentication was done via Google account and Google Multi Factor Authentication. Therefore, sampled accounts were found to be in line the requirements where MFA should be enabled for all users and administrators. Additionally, all cloud services make use of Google API login which depends on Google authentication. Two Mobile Device Management (MDM) was found to be utilise as well. ScaleFusion was found to be utilise in order to keep track with the software on the End User Devices (laptop) while Google MDM was used to keep track with mobile devices. Few issues was found during internal authenticate assessment where outdated software was found, however, this was resolved by updating the software to the latest version.

The assessor has concluded that Headhunter Systems T/A Gravyty has passed the required tests and should be awarded the Cyber Essentials Plus certification.

The Certificate number is 30a98f8c-ce74-4f89-b642-120a3928b03a and can be found at https://registry.blockmarktech.com/certificates/30a98f8c-ce74-4f89-b642-120a3928b03a/

The second certificate number is 8f632465-a205-4f29-b337-0e4938e9aef1 and can be found at https://registry.blockmarktech.com/certificates/8f632465-a205-4f29-b337-0e4938e9aef1/

If a test has not been passed successfully, the assessor has provided feedback within the relevant section.

Evidence of activities

In carrying out the audit, the assessor will have carried out a number of technical tests and have seen documentary evidence. This evidence forms a basis for the assessor's recommendations nd where appropriate has been included in this report.

Scope

The following networks and locations were considered in the scope of this assessment:

External perimeter only the website which is gravyty.com (35.188.155.232) Internal network segment during the internal authenticated scan was 10.10.10.0/24 Gravyty was based on Israel, Seattle and London

Any areas that were excluded from the audit are listed below:

None

Remote Vulnerability Assessment

The purpose of this test is to test whether an Internet-based opportunist attacker can hack into the applicant's system with typical low-skill

methods.

Each external IP address that is in scope has been scanned to identify any services that are open to the intenret. All open services are tested to confirm that they have met the requirements of Cyber Essentials.

This test was awarded PASS by the assessor

The test did not identify any vulnerabilities that were scored 7 or higher on CVSS v3 on the open services discovered during the testing of the external IP address.

All open services discovered were confirmed to be configured securely against the requirements as listed in Cyber Essentials.

This test was awarded PASS by the assessor

Internal Testing

A suitable set of devices that was selected at random by the assessor that is representative of 100% of the applicant infrastructure.

A summary of the breakdown of this sample is as follows:

List of inventory during the Cyber Essential Plus: Windows 11PRO 22h2: 75 Windows 10PRO 22h2: 35 android 13: 40+ android 14: 3 iOS iphone 16.7.2 - 52 iOS iphone 17.1.1 - 11 18 Mac books running version 14 (Sonoma) 2 Mac books running version 13.6 (Ventura) Sampled devices: Windows 11PRO 22h2: 5 Windows 10PRO 22h2: 4 android 13: 4 android 14: 2 iOS iphone 16.7.2 - 5 iOS iphone 17.1.1 - 3 3 Mac books running version 14 (Sonoma) 2 Mac books running version 13.6 (Ventura)

Check patching, by authenticated vulnerability scan of devices

The purpose of this test is to identify missing patches and security updates that leave vulnerabilities that threats within the scope of the scheme could easily exploit.

This test was awarded PASS by the assessor.

No vulnerabilities that were scored 7 or higher on CVSS v3, that could be remediated through applying a security update that was made available by a vendor more than 14 days ago, were discovered on the sampled devices.

Check Malware Protection

This test checks the sampled devices to confirm that all devices in scope benefit from a basic level of malware protection.

All devices and virtual desktop environments should either be using anti malware software or application allow listing.

This test was awarded PASS by the assessor.

All sampled devices have been tested and the assessor who has confirmed that they benefit from a basic level of malware protection.

For all devices using anti-malware software it has been confirmed that the software is functional and is being updated in line with vendor

recommendations.

For devices using application allow listing, the assessor has confirmed that the application allow list is configured correctly.

Check Multi-Factor Authentication (MFA) Configuration

All cloud services must be configured to authenticate using MFA. This test is in place to confirm that all cloud services that have been declared in the scope with MFA available are authenticating using MFA.

The assessor has checked the user of each sampled device against every cloud service that they use.

At least one administrator account and one standard user account has been checked for each cloud service.

This test was awarded PASS by the assessor

All users for sampled devices were observed authenticating to cloud services which they use as an organisational service and confirmed that they were authenticating using MFA.

At least one administrator and one standard user for each cloud service was tested.

Check Account Separation

This test is conducted to ensure that account separation is in place and that standard users can not conduct administrator tasks.

Elevating privileges is not an acceptable alternative to using separate accounts.

This test was awarded PASS by the assessor

The assessor has confirmed that all users of the sampled devices had standard user accounts and could not carry out an administrative task without entering credentials of a separate admin account.

Applicant Answers

	Applicant Answer	Assessor Score
A1.1 Organisation Name What is your organisation's name? **The answer given in A1.1 is the name that will be displayed on your certificate and has a character limit of 150.** When an organisation wishes to certify subsidiary companies on the same certificate, the organisation can certify as a group and can include the subsidiaries' name on the certificate as long as the board member signing off the certificate has authority over all certified organisations. For example: The Stationery Group, incorporating The Paper Mill and The Pen House. It is also possible to list on a certificate where organisations are trading as other names. For example: The Paper Mill trading as The Pen House.	Headhunter Systems T/A Gravyty	Compliant
A1.2 Organisation Type What type of organisation are you?	LTD - Limited Company (Ltd or PLC)	Compliant
A1.3 Organisation Number What is your organisation's registration number? Please enter the registered number only with **no spaces or other punctuation.** Letters (a-z) are allowed, but you need at least one digit (0-9). There is a 20 character limit for your answer. If you are applying for certification for more than one registered company, **please still enter only one organisation number.** If you have answered A1.2 with Government Agency, Sole Trader, Other Partnership, Other Club/Society or Other Organisation please enter "none". If you are registered in a country that does not issue a company number, please enter a unique identifier like a VAT or DUNS number.	07059614	Compliant
A1.4 Organisation Address	UK	Compliant

What is your organisation's address? Please provide the legal registered address for your organisation, if different from the main operating location.	Custom Fields: Address Line 1: 40 Anmersh Grove, Stanmore, Middx Town/City: Stanmore Postcode: HA7 1PA Country: United Kingdom	
A1.5 Organisation Occupation **What is your main business?** *Please summarise the main occupation of your organisation.*	IT Custom Fields: Applicant Notes: We are a Software development company with our own Suite of products for the Education and no profit market	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.*	gravyty.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 Reason for Certification **What are the two main reasons for applying for certification?** *Please let us know the two main reasons why you are applying for certification. If there are multiple reasons, please select the two that are most important to you. This helps us to understand how people are using our certifications.*	Required for Commercial Contract Custom Fields: Secondary Reason: To Give Confidence to Our Customers	Compliant
A1.8.1 Contracting Organisation **Who is the commercial contracting organisation?** *Please provide the name of the contracting organisation.*	Equal Education Partners	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. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*	Yes	Compliant
A1.10 Cyber Breach **Can IASME and their expert partners contact you if you experience a cyber breach?** *We would like feedback on how well the controls are protecting organisations. If you agree to this then please email security@iasme.co.uk if you do experience a cyber breach. IASME and expert partners will then contact you to find out a little more but all information will be kept confidential.*	Yes	Compliant
A2.1 Assessment Scope **Does the scope of this assessment cover your whole organisation?** **Please note: Your organisation is only eligible for free cyber insurance if your assessment covers your whole company, if you answer "No" to this question you will not be invited to apply for insurance.** *Your whole organisation includes all divisions, people and devices which access your organisation's data and services.*	Yes	Compliant
A2.3 Geographical Location **Please describe the geographical locations of your business which are in the scope of this assessment.** *You should provide either a broad description (i.e. All UK offices) or simply list the locations in scope (i.e. Manchester and Glasgow retail stores).*	Israel, Seattle and London	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.**	130 Lenovo notebooks running Windows 10 Pro 22H2 or Windows 11 Pro 22H2 and 20 Macbook Pros running Monterey or Ventura	Compliant Assessor Notes: devices running on windows 10 pro 21H2 require updating to be compliant

All user devices declared within the scope of the certification only require the make and operating system to be listed.We have removed the requirement for the applicant to list the model of the device.Devices that are connecting to cloud services must be included.A scope that does not include end user devices is not acceptable. *You need to provide a summary of all laptops, computers, virtual desktops and their operating systems that are used for accessing organisational data or services and have access to the internet.For example, "We have 25 DELL laptops running Windows 10 Professional version 20H2 and 10 MacBook laptops running MacOS Ventura".Please note, the edition and feature version of your Windows operating systems are required.This applies to both your corporate and user owned devices (BYOD). You do not need to provide serial numbers, mac addresses or further technical information.*		
A2.4.1 Thin Client Devices **Please list the quantity of thin clients within scope of this assessment. Please include make and operating systems.** *Please provide a summary of all the thin clients in scope that are connecting to organisational data or services (Definitions of which are in the 'CE Requirements for Infrastructure document' linked in question A1.9).* *Thin clients are commonly used to connect to a Virtual Desktop Solution.* ***Thin clients are a type of very simple computer holding only a base operating system which are often used to connect to virtual desktops. Thin clients can connect to the internet, and it is possible to modify some thin clients to operate more like PCs, and this can create security complications. Cyber Essentials requires thin clients be supported and receiving security updates.*** *https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*	N/A We have no Thin clients	Compliant
A2.5 Server Devices **Please list the quantity of servers, virtual servers and virtual server hosts (hypervisor). You must include the operating system.** *Please list the quantity of all servers within scope of this assessment.*	None -using Google Cloud - Google Workspace and have no on prem servers for our operations. All the other servers are specific to our products we develop and not in scope.	Compliant

For example, 2 x VMware ESXI 6.7 hosting 8 virtual windows 2016 servers; 1 x MS Server 2019; 1 x Redhat Enterprise Linux 8.3		
A2.6 Mobile Devices Please list the quantities of tablets and mobile devices within the scope of this assessment. **Please Note** You must include make and operating system versions for all devices. All user devices declared within the scope of the certification only require the make and operating system to be listed. We have removed the requirement for the applicant to list the model of the device. **Devices that are connecting to cloud services must be included in scope that does not include end user devices is not acceptable.** *All tablets and mobile devices that are used for accessing organisational data or services and have access to the internet must be included in the scope of the assessment. This applies to both corporate and user owned devices (BYOD).You are not required to list any serial numbers, mac addresses or other technical information.*	55 x iPhone running iOS 16.3.1 or 16.6.1 or 17.0.1/2/3 10x Android 14.X 30x Android 13.X 10x Android 12.X 5x Android 11.X 235271	Compliant Assessor Notes: answer must include the iOS of the iphones
A2.7 Networks **Please provide a list of your networks that will be in the scope for this assessment.** *You should include details of each network used in your organisation including its name, location and its purpose (i.e. Main Network at Head Office for administrative use, Development Network at Malvern Office for testing software, home workers network - based in UK).* *You do not need to provide IP addresses or other technical information.* *For further guidance see the Home Working section in the 'CE Requirements for Infrastructure Document'.* https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf	All our networks in the Israel, London and Seattle offices are of an Ad-hoc basis with UTM devices protecting the access points	Compliant
A2.7.1 Home Workers **How many staff are home workers?**	43	Compliant Assessor Notes: answer only requires the number of

Any employee that has been given permission to work at home for any period of time at the time of the assessment, needs to be classed as working from home for Cyber Essentials. *For further guidance see the Home Working section in the 'CE Requirements for Infrastructure Document'.* *https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*		home workers, this is anyone that has permission to work from home. Answer needs to be updated to only contain this as home workers can not be out of scope
A2.8 Network Equipment **Please provide a list of your network equipment that will be in scope for this assessment (including firewalls and routers). You must include make and model of each device listed.** *You should include all equipment that controls the flow of data, this will be your routers and firewalls.* *You do not need to include switches or wireless access points that do not contain a firewall or do not route internet traffic.* *If you don't have an office and do not use network equipment, instead you are relying on software firewalls please describe in the notes field.* *You are not required to list any IP addresses, MAC addresses or serial numbers.*	Fortigate 100E firewall and principal router. Connectivity through two (2) HP switches with 48 ports each and eight (8) Netgear access points with WPA 2.0 encryption.	Compliant
A2.9 Cloud Services Please list all of your cloud services that are in use by your organisation and provided by a third party. **Please note cloud services cannot be excluded from the scope of CE.** *You need to include details of all of your cloud services. This includes all types of services - IaaS, PaaS and SaaS. Definitions of the different types of Cloud Services are provided in the 'CE Requirements for Infrastructure Document'.* https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf	Google Workspace, Office 365, AWS, MongoDB, Sendgrid, Google Analytics, Google Developers, Salesforce, Raisers Edge NXT	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**	Elad Avni Custom Fields: Responsible Person Role: IT Director	Compliant

assessment. *This person must be a member of your organisation and cannot be a person employed by your outsourced IT provider.*		
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-Out	Compliant
A4.1 Boundary Firewall **Do you have firewalls at the boundaries between your organisation's internal networks, laptops, desktops, servers and the internet?** *You must have firewalls in place between your office network and the internet.*	Yes	Compliant
A4.1.1 Off Network Firewalls **When your devices (including computers used by homeworkers) are being used away from your workplace (for example, when they are not connected to your internal network), how do you ensure they are protected?** You should have firewalls in place for home-based workers. If those users are not using a Corporate Virtual Private Network (VPN) connected to your office network, they will need to rely on the software firewall included in the operating system of their device.	Home works all have software based Firewalls in place	Compliant
A4.2 Firewall Default Password	Yes	Compliant

When you first receive an internet router or hardware firewall device, it may have had a default password on it. Have you changed all the default passwords on your boundary firewall devices? *The default password must be changed on all routers and firewalls, including those that come with a unique password pre-configured (i.e. BT Business Hub, Draytek Vigor 2865ac).* *When relying on software firewalls included as part of the operating system of your end user devices, the password to access the device will need to be changed.*		
A4.2.1 Firewall Password Change Process **Please describe the process for changing your firewall password?** **Home routers not supplied by your organisation are not included in this requirement.** *You need to understand how the password on your firewall(s) is changed. Please provide a brief description of how this is achieved.*	Old password is removed, password requirement is set to very high and new random password is generated with a minimum of 12 characters including a minimum of 1 Capital letter, 1 number and 1 special character. 1) Authorised person with credentials logs into the admin console 2) they go to the password settings 3) Change the password to a randomly generated new password that conforms to a minimum of 12 characters, Alpha numeric with a special character and a capital letter. 4) Saves the changes.	Compliant Assessor Notes: please describe the process for example, log on to the admin console and the password is changed to .....
A4.3 Firewall Password Configuration Is your new firewall password configured to meet the 'Password-based authentication' requirements? Please select the option being used. A. Multi-factor authentication, with a minimum password length of 8 characters and no maximum length B. Automatic blocking of common passwords, with a minimum password length of 8 characters and no maximum length C. A minimum password length of 12 characters and no maximum length D. None of the above, please describe *Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the new section about password-based authentication in the 'Cyber Essentials Requirements for IT Infrastructure' document.* https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf	0: C. A password minimum length of 12 characters and no maximum length	Compliant

A4.4 Firewall Password Issue **Do you change your firewall password when you know or suspect it has been compromised?** *Passwords may be compromised if there has been a virus on your system or if the manufacturer notifies you of a security weakness in their product. You should be aware of this and know how to change the password if this occurs.* *When relying on software firewalls included as part of the operating system of your end user devices, the password to access the device will need to be changed.*	Yes	Compliant
A4.5 Firewall Services **Do you have any services enabled that can be accessed externally through your internet router, hardware firewall or software firewall?** *At times your firewall may be configured to allow a system on the inside to become accessible from the internet (for example: a VPN server, a mail server, an FTP server or a service that is accessed by your customers). This is sometimes referred to as "opening a port". You need to show a business case for doing this because it can present security risks. If you have not enabled any services, answer "No". By default, most firewalls block all services.*	No	Compliant
A4.7 Firewall Service Block **Have you configured your boundary firewalls so that they block all other services from being advertised to the internet?** *By default, most firewalls block all services from inside the network from being accessed from the internet, but you need to check your firewall settings.*	Yes	Compliant
A4.8 Firewall Remote Configuration **Are your boundary firewalls configured to allow access to their configuration settings over the internet?** *Sometimes organisations configure their firewall to allow other people (such as an IT support company) to change the settings via the internet.*	Yes Custom Fields: Applicant Notes: Our firewall is supplied by the ISP and as such is remotely managed	Compliant

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.		
A4.9 Documented Admin Access **If you answered yes in question A4.8, is there a documented business requirement for this access?** *When you have made a decision to provide external access to your routers and firewalls, this decision must be documented (for example, written down).*	Yes	Compliant
A4.10 Admin Access Method **If you answered yes in question A4.8, is the access to your firewall settings protected by either multi-factor authentication or by only allowing trusted IP addresses combined with managed authentication to access the settings?** *If you allow direct access to configuration settings via your router or firewall's external interface, this must be protected by one of the two options.* *Please explain which option is used.*	Access is via a trusted IP and multi factor authentication.	Compliant
A4.11 Software Firewalls **Do you have software firewalls enabled on all of your computers, laptops and servers?** *Your software firewall must be configured and enabled at all times, even when sitting behind a physical/virtual boundary firewall in an office location. You can check this setting on Macs in the Security & Privacy section of System Preferences. On Windows laptops you can check this by going to Settings and searching for "Windows firewall". On Linux try "ufw status".*	Yes	Compliant
A5.1 Removed Unused Software **Where you are able to do so, have you removed or disabled all the software and services that you do not use on your laptops, desktop computers, thin clients, servers, tablets, mobile phones and cloud services? Describe how you**	Yes	Compliant

achieved this. *You must remove or disable all applications, system utilities and network services that are not needed in day-to-day use. You need to check your cloud services and disable any services that are not required for day-to-day use.* *To view your installed applications:* *1. Windows by right clicking on Start ? Apps and Features* *2. macOS open Finder -> Applications* *3. Linux open your software package manager (apt, rpm, yum).*		
A5.2 Remove Unrequired User Accounts **Have you ensured that all your laptops, computers, servers, tablets, mobile devices and cloud services only contain necessary user accounts that are regularly used in the course of your business?** *You must remove or disable any user accounts that are not needed in day-to-day use on all devices and cloud services.* *You can view your user accounts* *1. Windows by righting-click on Start -> Computer Management -> Users,* *2. macOS in System Preferences -> Users & Groups* *3. Linux using ""cat /etc/passwd""*	Yes	Compliant
A5.3 Change Default Password **Have you changed the default password for all user and administrator accounts on all your desktop computers, laptops, thin clients, servers, tablets and mobile phones that follow the Password-based authentication requirements of Cyber Essentials?** *A password that is difficult to guess will be unique and not be made up of common or predictable words such as "password" or "admin" or include predictable number sequences such as "12345".*	Yes	Compliant
A5.4 Internally Hosted External Services **Do you run external services that provides access to data (that shouldn't be made public) to users across the internet?** *Your business might run software that*	No	Compliant

allows staff or customers to access information across the internet to an external service hosted on the internal network, cloud data centre or IaaS cloud service. This could be a VPN server, a mail server, or an internally hosted internet application(SaaS or PaaS) that you provide to your customers as a product. In all cases, these applications provide information that is confidential to your business and your customers and that you would not want to be publicly accessible.		
A5.8 Auto-Run Disabled **Is "auto-run" or "auto-play" disabled on all of your systems?** This is a setting on your device which automatically runs software on external media or downloaded from the internet. *It is acceptable to choose the option where a user is prompted to make a choice about what action will occur each time they insert a memory stick. If you have chosen this option, you can answer yes to this question.*	Yes	Compliant
A5.9 Device Locking **When a device requires a user to be present, do you set a locking mechanism on your devices to access the software and services installed?** *Device locking mechanisms such as biometric, password or PIN, need to be enabled to prevent unauthorised access to devices accessing organisational data or services.*	Yes	Compliant
A5.10 Device Locking Method **Which method do you use to unlock the devices?** Please refer to Device Unlocking Credentials paragraph found under Secure Configuration in the Cyber Essentials Requirements for IT Infrastructure document for further information. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf The use of a PIN with a length of at least six characters can only be used where the credentials are just to unlock a device and does not provide access to	We use secure password linked to Google and rotated regularly. as well as biometrics. Devices are connected to Google Workspace and use a MDM. To unlock a device, the user must log in via their Google workspace credentials which has an enforced Multi Factor authentication via an accredited Authenticator app and requires a strong password associated with the account with a minimum of 16 characters. (alpha-numeric + special character + capital letter and not a re-used password from the last 12 months) We also have a deny list in place for passwords that are to common	Compliant

organisational data and services without further authentication.		
A6.1 Supported Operating System **Are all operating systems on your devices supported by a vendor that produces regular security updates?** **If you have included firewall or router devices in your scope, the firmware of these devices is considered to be an operating system and needs to meet this requirement.** *Older operating systems that are out of regular support include Windows 7/XP/Vista/ Server 2003, mac OS Mojave, iOS 12, iOS 13, Android 8 and Ubuntu Linux 17.10.* *It is important you keep track of your operating systems and understand when they have gone end of life (EOL). Most major vendors will have published EOL dates for their operating systems and firmware.*	Yes Custom Fields: Applicant Notes: As per previous notes, all OS are auto updated and managed by MDM to ensure that they are immediately updated to the latest vendor version / patch release	Compliant Assessor Notes: not compliant due to other answers that require updating
A6.2 Supported Software **Is all the software on your devices supported by a supplier that produces regular fixes for any security problems?** *All software used by your organisation must be supported by a supplier who provides regular security updates. Unsupported software must be removed from your devices. This includes frameworks and plugins such as Java, Adobe Reader and .NET.*	Yes	Compliant
A6.2.1 Internet Browsers **Please list your internet browser(s). The version is required.** *Please list all internet browsers installed on your devices, so that the Assessor can understand your setup and verify that they are in support.* *For example: Chrome Version 102, Safari Version 15.*	Chrome Version 117.0.5938.XX Safari version 16.5 Firefox 117.0.1 only for developer testing	Compliant
A6.2.2 Malware Protection **Please list your Malware Protection software.** **The version is required.**	Windows defender Sentinel One 22.3.5.887	Compliant

Please list all malware protection and versions you use so that the Assessor can understand your setup and verify that they are in support. *For example: Sophos Endpoint Protection V10, Windows Defender, Bitdefender Internet Security 2020.*		
A6.2.3 Email Application **Please list your email applications installed on end user devices and server. The version is required.** *Please list all email applications and versions you use so that the Assessor can understand your setup and verify that they are in support.* *For example: MS Exchange 2016, Outlook 2019.*	None. We use Gmail in the cloud	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.*	MS Office 365 Google Workspace	Compliant
A6.3 Software Licensing **Is all software licensed in accordance with the publisher's recommendations?** *All software must be licensed. It is acceptable to use free and open source software as long as you comply with any licensing requirements.* *Please be aware that for some operating systems, firmware and applications, if annual licensing is not purchased, they will not be receiving regular security updates.*	Yes	Compliant
A6.4 Security Updates - Operating System **Are all high-risk or critical security updates for operating systems and router and firewall firmware installed within 14 days of release?**	Yes	Compliant

You must install all high and critical security updates within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question. You are not required to install feature updates or optional updates in order to meet this requirement. *This requirement includes the firmware on your firewalls and routers.*		
A6.4.1 Auto Updates - Operating System **Are all updates applied for operating systems by enabling auto updates?** *Most devices have the option to enable auto updates. This must be enabled on any device where possible.*	Yes Custom Fields: Applicant Notes: Managed by MDM	Compliant
A6.4.2 Manual Updates - Operating System **Where auto updates are not being used, how do you ensure all high-risk or critical security updates of all operating systems and firmware on firewalls and routers are applied within 14 days of release?** *It is not always possible to apply auto updates, this is often the case when you have critical systems or servers and you need to be in control of the updating process.* *Please describe how any updates are applied when auto updates are not configured.* *If you only use auto updates, please confirm this in the notes field for this question.*	We have rolled out device management software to force all machines to auto update daily. We have set a threshold to ensure that if a user does not comply with the required restart for an update within 10 days of release the MDM alerts them that the machine will auto reboot in order to install the required patches to remain compliant. Our IT Team and Core operations team receive regular alerts / reports so they can ensure that this is all happening as per the programming. enforced by MDM	Compliant Assessor Notes:
A6.5 Security Updates - Applications **Are all high-risk or critical security updates for applications (including any associated files and any plugins such as Java, Adobe Reader and .Net.) installed within 14 days of release?** *You must install any such updates within 14 days in all circumstances.* *If you cannot achieve this requirement at all times, you will not achieve compliance to this question.* *You are not required to install feature updates or optional updates in order to meet this requirement, just high-risk or critical security updates.*	Yes Custom Fields: Applicant Notes: Managed by MDM	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.*	Yes Custom Fields: Applicant Notes: Enforced and Managed by MDM	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 of all applications are applied within 14 days of release?** *It is not always possible to apply auto updates, this is often the case when you have critical systems or applications and you need to be in control of the updating process.* *Please describe how any updates are applied when auto updates are not configured.* *If you only use auto updates, please confirm this in the notes field for this question.*	Auto updates are in place and managed by a MDM to ensure all updates are installed within 14 days of release and all High-risk or critical security patches are installed immediately. For any outlier devices and applications that cannot be auto updated the MDM that is in place sends alerts / Reports to the IT director to ensure that the IT team address all high risk and critical updates within a window period of a few days. The reports are generated daily to ensure that nothing that required a high risk or critical update is left for more than a day or two and all other updates are completed within a two week period.	Compliant Assessor Notes: answer must include high-risk or critical security updates. also must include how you ensure this is done within 14 days
A6.6 Unsupported Software Removal **Have you removed any software installed on your devices that is no longer supported and no longer receives regular updates for security problems?** *You must remove older software from your devices when it is no longer supported by the manufacturer. Such software might include older versions of web browsers, operating systems, frameworks such as Java and Flash, and all application software.*	Yes	Compliant
A6.7 Unsupported Software Segregation **Where you have a business need to use unsupported software, have you moved the devices and software out of scope of this assessment? Please explain how you achieve this.** *Software that is not removed from devices when it becomes un-supported will need to be placed onto its own sub-set with no internet access.* *If the out-of-scope subset remains connected to the internet, you will not be able to achieve whole company certification and an excluding statement will be required in question A2.2.* *A sub-set is defined as a part of the organisation whose network is*	We do not use unsupported software.	Compliant

segregated from the rest of the organisation by a firewall or VLAN.		
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.*	We have an onboarding and offboarding process whereby any new employee gets onboarded via HR and depending on their role, the system is configures to send a request to IT for a computer to be set up for them with the relevant software and permissions. The same is true for offboarding	Compliant
A7.2 Unique Accounts **Are all your user and administrative accounts accessed by entering a unique username and password?** *You must ensure that no devices can be accessed without entering a username and password.* **Accounts must not be shared.**	Yes	Compliant
A7.3 Leavers Accounts **How do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation?** *When an individual leaves your organisation you need to stop them accessing any of your systems.*	Our offboard process removes all access an privileges when a person leaves the company.	Compliant
A7.4 User Privileges **Do you ensure that staff only have the privileges that they need to do their current job? How do you do this?** *When a staff member changes job role, you may also need to change their permissions to only access the files, folders and applications that they need to do their day to day work.*	Each role has a defined scope and it is defines what services they have access levels per individual. This is then managed by the IT team, Core Director and VP of Engineering who have admin permissions to ensure that only relevant individuals have elevated access if they require and to remove this access when no longer required.	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*	For anyone requiring administrator access, they need to put in a support ticket asking for the relevant access. Said request is then escalated to the Vice President of Technology to approve and grant the relevant access at his discretion.	Compliant Assessor Notes: who approves the access?

to systems at administrator level. This process might include approval by a person who is an owner/director/trustee/partner of the organisation.		
A7.6 Use of Administrator Accounts **How does your organisation make sure that separate accounts are used to carry out administrative tasks (such as installing software or making configuration changes)?** *You must use a separate administrator account from the standard user account, when carrying out administrative tasks such as installing software. Using administrator accounts all-day-long exposes the device to compromise by malware. Cloud service administration must be carried out through separate accounts.*	This is done via permissions and education as required.	Compliant
A7.7 Managing Administrator Account Usage **How does your organisation prevent administrator accounts from being used to carry out every day tasks like browsing the web or accessing email?** *This question relates to the activities carried out when an administrator account is in use.* *You must ensure that administrator accounts are not used to access websites or download email. Using such accounts in this way exposes the device to compromise by malware. Software and update downloads should be performed as a standard user and then installed as an administrator. You might not need a technical solution to achieve this, it could be based on good policy, procedure and regular training for staff.*	To ensure that Administrator accounts are not used for daily task, we provide the users with training and education on the dangers of using an admin account for general tasks as well as covering the company policy of the use of Admin accounts for general browsing, email, downloads etc with refresher training run for all new hires and yearly to ensure compliance by the team.	Compliant Assessor Notes: how do you ensure these are not used for daily tasks such as accessing websites etc? this can be through separate accounts without internet access, training etc
A7.8 Administrator Account Tracking **Do you formally track which users have administrator accounts in your organisation?** *You must track all people that have been granted administrator accounts.*	Yes Custom Fields: Applicant Notes: ONLY IT Team	Compliant
A7.9 Administrator Access Review **Do you review who should have administrative access on a regular basis?**	Yes Custom Fields: Applicant Notes:	Compliant

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.	except IT employees, it is done on an ad-hoc basis weekly as per requirements	
A7.10 Brute Force Attack Protection **Describe how you protect accounts from brute-force password guessing in your organisation?** *A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.* *Information on how to protect against brute-force password guessing can be found in the Password-based authentication section, under the User Access Control section in the 'Cyber Essentials Requirements for IT Infrastructure* *https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*	EDR is enabled on laptops & All Google accounts are required to change passwords every 3 months and we enforce multi factor authentication on all accounts.	Compliant
A7.11 Password Quality **Which technical controls are used to manage the quality of your passwords within your organisation?** *Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the new section about password-based authentication in the 'Cyber Essentials Requirements for IT Infrastructure' document.* *https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*	Password control is set up in Google Workspace requiring a minimum of 16 characters, with a specials character, a capital letter and a number. Rotation of passwords is enforces and we do not allow the reusing passwords in a 12 month period all this MFA enabled.	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.*	We use Google Workplace to enforce the secure, strong and unique passwords by not allowing weak passwords and the reuse of old passwords and common passwords.	Compliant

Further information can be found in the password-based authentication section, under the User Access Control section in the Cyber Essentials Requirements for IT Infrastructure document. *https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf*		
A7.13 Password Policy **Do you have a process for when you believe the passwords or accounts have been compromised?** *You must have an established process that details how to change passwords promptly if you believe or suspect a password or account has been compromised.*	Yes	Compliant
A7.14 MFA Enabled **Do all of your cloud services have multi-factor authentication (MFA) available as part of the service?** *Where your systems and cloud services support multi-factor authentication (MFA), for example, a text message, a one time access code, notification from an authentication app, then you must enable for all users and administrators. For more information see the NCSC's guidance on MFA.* *Where a cloud service does not have its own MFA solution but can be configured to link to another cloud service to provide MFA, the link will need to be configured. A lot of cloud services use another cloud service to provide MFA. Examples of cloud services that can be linked to are Azure, MS365, Google Workspace.*	Yes	Compliant
A7.16 Administrator MFA **Has MFA been applied to all administrators of your cloud services?** *It is required that all administrator accounts on cloud service must apply multi-factor authentication in conjunction with a password of at least 8 characters.*	Yes	Compliant
A7.17 User MFA **Has MFA been applied to all users of your cloud services?** *All users of your cloud services must use*	Yes	Compliant

MFA in conjunction with a password of at least 8 characters.		
A8.1 Malware Protection **Are all of your desktop computers, laptops, tablets and mobile phones protected from malware by either:** **A - Having anti-malware software installed** **and/or** **B - Limiting installation of applications by application allow listing (For example, using an app store and a list of approved applications, using a Mobile Device Management(MDM solution)** **or** **C - None of the above, please describe** Please select all the options that are in use in your organisation across all your devices. Most organisations that use smartphones and standard laptops will need to select both option A and B. Option A - option for all in-scope devices running Windows or macOS including servers, desktop computers; laptop computers Option B - option for all in-scope devices Option C - none of the above, explanation notes will be required.	0: A - Anti-Malware Software, 1: B - Limiting installation of applications by application allow listing from an approved app store	Compliant
A8.2 Daily Update **If Option A has been selected: Where you have anti-malware software installed, is it set to update in line with the vendor's guidelines and prevent malware from running on detection?** *This is usually the default setting for anti-malware software. You can check these settings in the configuration screen for your anti-malware software. You can use any commonly used anti-malware product, whether free or paid-for as long as it can meet the requirements in this question. For the avoidance of doubt, Windows Defender is suitable for this purpose.*	Yes	Compliant
A8.3 Scan Web Pages **If Option A has been selected: Where you have anti-malware software installed, is it set to scan web pages you visit and warn you about accessing malicious websites?** *Your anti-malware software or internet*	Yes	Compliant

browser should be configured to prevent access to known malicious websites. On Windows 10, SmartScreen can provide this functionality.		
A8.4 Application Signing **If Option B has been selected: Where you use an app-store or application signing, are users restricted from installing unsigned applications?** *Some operating systems which include Windows S, Chromebooks, mobile phones and tablets restrict you from installing unsigned applications. Usually you have to "root" or "jailbreak" a device to allow unsigned applications.*	Yes	Compliant
A8.5 Approved Application List **If Option B has been selected: Where you use an app-store or application signing, do you ensure that users only install applications that have been approved by your organisation and do you maintain this list of approved applications?** *You must create a list of approved applications and ensure users only install these applications on their devices. This includes employee-owned devices. You may use mobile device management (MDM) software to meet this requirement but you are not required to use MDM software if you can meet the requirements using good policy, processes and training of staff.*	Yes	Compliant
Acceptance Please read these terms and conditions carefully. Do you agree to these terms? NOTE: if you do not agree to these terms, your answers will not be assessed or certified.	I accept	Compliant