Cyber Essentials Scheme

Applicant: Tachart,

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

Congratulations, you have been successful in your assessment under the Cyber Essentials scheme.

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

Question	Answer	Score	Comments
Acceptance Please read these terms and conditions carefully. Do you agree to these terms? NOTE: if you do not agree to these terms, your answers will not be assessed or certified.	I accept	Compliant	
A1.1 Organisation Name What is your organisation's name (for companies: as registered with Companies House)? Please provide the full name for the company being certified. If you are certifying the local entity of a multinational company, provide the name of the local entity.	TACHART LIMITED	Compliant	
A1.2 Organisation Number What is your organisation's registration number (if you have one)? If you are a UK limited company, your registration number will be provided by Companies House, in the Republic of Ireland, this will be provided by Companies Registration Office. Charities, partnerships and other organisations should provide their registration number if applicable.	01329903	Compliant	
A1.3 Organisation Address Where are you located? Please provide the legal registered address for your organisation, or your trading address if a sole trader.	UK Address Line 1: Bnm Building Whitelea Road Swinton Town/City: Mexborough County: S Yorkshire Postcode: S64 8BH	Compliant	
A1.4 Type of Organisation What is your main business? Please summarise the main occupation of your organisation.	Manufacturing	Compliant	
A1.5 Website What is your website address? Please provide your website address (if you have one). This can be a Facebook/Linkedin page if you prefer.	https://www.tachart.com/	Compliant	

Question	Answer	Score	Comments
A1.6 Size of Organisation What is the size of your organisation? Based on the EU definitions of Micro (<10 employees, < €2m turnover), Small (<50 employees, < €10m turnover) , Medium (<250 employees, < €50m turnover) or Large (>250 Employees or >€50m turnover).	Small (<50 Employees and <€10m Turnover)	Compliant	
A1.7 Home Workers How many staff are home workers? Home workers are staff whose main work location is their home address and who work there for the majority of their time. This does not include office workers who occasionally work at home or when traveling.	None	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 would include all divisions and all people and devices that use business data.	Yes	Compliant	
A2.5 Geographic 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).	Single site located on Whitelea Road, Swinton, UK	Compliant	

Question	Answer	Score	Comments
A2.6 Devices Please provide a summary of all laptops, computers and servers that are used for accessing business data and have access to the internet (for example, "We have 25 laptops running Windows 10 version 1709 and 10 MacBook Air laptops running macOS Mojave"). You do not need to provide serial numbers, mac addresses or further technical information. It is essential to include the version number for Windows 10 - the assessor will be unable to mark the assessment without this.	1 server 2012, 3 Windows 7 computers, 1 Windows 10 computer and 3x Windows XP comuters, The Windows XP machines are out of scope as are dicconected from the network and are used for running CNC machines only so dont contain any business data.	Compliant	
A2.7 Mobile Devices Please list the quantities of tablets and mobile devices within the scope of this assessment. You must include model and operating system version for all devices. All tablets and mobile devices that are used for accessing business data and have access to the internet must be included in the scope of the assessment. You do not need to provide serial numbers, mac addresses or other technical information.	1 Android phones, version 8 2 iphones, version Ios13	Compliant	
A2.8 Networks Please provide a list of the 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). You do not need to provide IP addresses or other technical information.	main LAN located at the site office. No remote networks and no home users.	Compliant	

Question	Answer	Score	Comments
A2.9 Network Equipment Please provide a list of network equipment that will be in scope for this assessment (including firewalls and routers). You should include all equipment that controls the flow of data such as 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.	1x Draytek router which is acting as the switch also.	Compliant	
A2.10 Responsible Person Please provide the name and role of the person who is responsible for managing the information systems in the scope of this assessment? This should be the person who influences and makes decisions about the computers, laptops, servers, tablets, mobile phones and network equipment within your organisation. This person must be a member of your organisation and cannot be a person employed by your outsourced IT provider.	Dean Lancashire	Compliant	
A4.1 Firewalls Do you have firewalls at the boundaries between your organisation's internal networks and the internet? You must have firewalls in place between your office network and the internet. You should also have firewalls in place for home-based workers, if those users are not using a Virtual Private Network (VPN) connected to your office network.	Yes Applicant Notes: Yes, the draytek router is our main firewall.	Compliant	

Question	Answer	Score	Comments
A4.2 Change Default Password When you first receive an internet router or hardware firewall device it will have had a default password on it. Has this initial password been changed on all such devices? How do you achieve this? The default password must be changed on all routers and firewalls, including those that come with a unique password pre-configured (i.e. BT Hub) You can change the default password by logging into the web interface for the device (often located at 192.168.1.1 or 192.168.1.254)	When new network Hardware is purchased, per-config work is performed by IT Desk. This includes changing the default password to a strong 12 character long one and disabling any unnecessary features.	Compliant	
A4.3 Password Quality Is the new password on all your internet routers or hardware firewall devices at least 8 characters in length and difficult to guess? 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 Applicant Notes: Yes, all passwords are set as per our security policy which states that passwords need to be complex and difficult to guess and over 8 chars	Compliant	
A4.4 Password Management Do you change the password when you believe it may have been compromised? How do you achieve this? 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 we believe a password has been compromised, we notify IT Desk. From there IT Desk reset the password immediately to a strong one and check if any other services use that password, if any do, they will reset those also.	Compliant	

Question	Answer	Score	Comments
A4.5 Services Enabled Do you have any services enabled that are accessible externally from your internet routers or hardware firewall devices for which you do not have a documented business case? At times your firewall may be configured to allow a system on the inside to become accessible from the internet (such as a VPN server, a mail 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. The business case should be documented and recorded.	No Applicant Notes: yes, all external services are disabled by IT Desk. This is reviewed periodically.	Compliant	
A4.7 Service Blocking Have you configured your internet routers or hardware firewall devices 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 Applicant Notes: Yes, the firwall dosent advertise any services to the internet. this is set by IT Desk.	Compliant	
A4.8 Configuration Settings Are your internet routers or hardware firewalls configured to allow access to their configuration settings over the internet? Sometimes organisations configure their firewall to allow other people (such as an IT support company) to change the settings via the internet. If you have not set up your firewalls to be accessible to people outside your organisations or your device configuration settings are only accessible via a VPN connection, then answer 'no' to this question.	No Applicant Notes: Yes, our router firewall can only be accessed internally. All remote access to configuration is disabled.	Compliant	

Question	Answer	Score	Comments
A4.11 Software Firewalls Do you have software firewalls enabled on all of your computers and laptops? 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'. You can also use the firewall that may be provided by your anti-virus software.	Yes Applicant Notes: yes, the buit in Windows firewall is enabled on all computers.	Compliant	
A5.1 Remove Unused Software Where you are able to do so, have you removed or disabled all the software that you do not use on your laptops, computers, servers, tablets and mobile phones? Describe how you achieve this. To view your installed applications on Windows look in Start Menu, on macOS open Finder -> Applications and on Linux open your software package manager (apt, rpm, yum). You must remove or disable all applications, system utilities and network services that are not needed in day-to-day use.	Yes, all unneccessary software has been removed. We review authorised software periodically and request IT Desk to remove unused applications.	Compliant	
A5.2 Necessary User Accounts Have you ensured that all your laptops, computers, servers, tablets and mobile devices 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 no needed in day-to-day use on all devices. You can view your user accounts on Windows by righting-click on Start -> Computer Management -> Users, on macOS in System Preferences -> Users & Groups, and on Linux using 'cat /etc/passwd'.	Yes Applicant Notes: Yes, all unneeded and stale user accounts have been removed. Our offboarding process also contains line items which require IT Desk to remove user accounts and profiles from PC's when a staff member leaves the company.	Compliant	

Question	Answer	Score	Comments
A5.3 Change Default Password Have you changed the default password for all user and administrator accounts on all your laptops, computers, servers, tablets and smartphones to a non-guessable password of 8 characters or more? 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 Applicant Notes: Yes. Our security policy specifies the need to use strong passwords. IT Desk also use group policy and checks their side to ensure that all passwords are strong, are over 8 chars long and non guessable. All phones have password over 8 chars and non guessable also.	Compliant	
A5.4 Password Quality Do all your users and administrators use passwords of at least 8 characters? The longer a password, the more difficult it is for cyber criminals to guess (or brute-force) it.	Yes Applicant Notes: yes. all users and admin use strong passwords (over 8 chars) in line with our security policy	Compliant	
A5.5 Sensitive or Critical Information Do you run software that provides sensitive or critical information (that shouldn't be made public) to external users across the internet? Your business might run software that allows people outside the company on the internet to access information within your business via an external service. This could be a VPN server, a mail server, or an internet application that you provide to your customers as a product. In all cases these applications provide information is confidential to your business and your customers and that you would not want to be publicly accessible. This question does not apply to cloud services such as Google Drive, Office365 or Dropbox. If you only use such services and do not run your own service you should answer no to this question.	No	Compliant	

Question	Answer	Score	Comments
A5.10 Auto-Run Disabled Is 'auto-run' or 'auto-play' disabled on all of your systems? This is a setting which automatically runs software on a DVD or memory stick. You can disable 'auto-run' or 'auto-play' on Windows through Settings, on macOS through System Preferences and on Linux through the settings app for your distribution. 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	
A6.1 Operating System Supported Are all operating systems and firmware on your devices supported by a supplier that produces regular fixes for any security problems? Please list the operating systems you use so that the assessor can understand you setup and verify that all your operating systems are still in support. Older operating systems that are out of support include Windows XP/Vista/2003, mac OS El Capitan and Ubuntu Linux 17.10	Machines that run on outdated software (such as Windows XP) are not connected to the network, do not have internet capability, do not contain any business data and are standalone machines that are used to manage CNC machinery within the plant. A standalone Laptop is used by the accounts dept, for the printing of payslips and is not connected to the network. Other than that all devices which are in scope are supported by suppliers who produce regular security fixes.	Compliant	
A6.2 Applications Supported Are all applications on your devices supported by a supplier that produces regular fixes for any security problems? Please summarise the applications you use so the assessor can understand your setup and confirm that all applications are supported. This includes frameworks and plugins such as Java, Flash, Adobe Reader and .NET	Yes, all applications are covered by their own support. We dont use any outdated or unsupported software.	Compliant	

Question	Answer	Score	Comments
A6.3 Software Licensed 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.	Yes	Compliant	
A6.4 Security Updates - Operating System Are all high-risk or critical security updates for operating systems and firmware installed within 14 days of release? Describe how do you achieve this. 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.	IT Desk have installed remote monitoring agents on all devices that links to their RMM solution. This monitors current OS patch level and firmware version. This agent also installs security updates for the OS automatically and notifies when firmware needs updating which IT Desk act on when released. Checks are done twice a week and updated within 14 days.	Compliant	
A6.5 Security Updates - Applications Are all high-risk or critical security updates for applications (including any associated files and any plugins such as Adobe Flash) installed within 14 days of release? Describe how you achieve this. 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.	The remote monitoring agent mentioned in question 41 also does same for third party applications. Checks are done twice a week and updated within 14 days.	Compliant	

Question	Answer	Score	Comments
A6.6 Unsupported Applications Have you removed any applications on your devices that are no longer supported and no longer received regular fixes for security problems? You must remove older applications from your devices when they are no longer supported by the manufacturer. Such applications might include older versions of web browsers, frameworks such as Java and Flash, and all application software.	Yes Applicant Notes: yes, we have a policy in place to check and remove appluications which fall outside their suppliers support. IT Desk do this for us.	Compliant	
A7.1 Account Creation Are 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.	Yes, We send a support ticket to IT Desk for when a user needs to be created. This will include what accounts they require (Domain Login, Email Account etc) which folder shares they are require access to and any specific software they need installing on their workstation.	Compliant	
A7.2 Unique Login Can you only access laptops, computers and servers in your organisation (and the applications they contain) by entering a unique user name and password? You must ensure that no devices can be accessed without entering a username and password. Users cannot share accounts.	Yes Applicant Notes: Yes	Compliant	
A7.3 Leavers Account Management How do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation? When an individual leaves your organisation you need to stop them accessing any of your systems.	We have an offboarding process which ensures that all staff who leave the company have their accounts disabled. We also perform a routine check on accounts to ensure that they are still required. IT Desk do this for us.	Compliant	

Question	Answer	Score	Comments
A7.4 Staff 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 access privileges to systems and data.	Yes. Dean at our side is the only person who can authorise security changes. This is done by raising a security change ticket with IT Desk. We reguilary review the permissions that the differnet team members have to ensure that noone has security access which contradicts their job role.	Compliant	
A7.5 Administrator Process Do you have a formal process for giving someone access to systems at an “administrator” level? Describe the process. You must have a formal, written-down 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.	Yes. only IT desk have admin access to our systems. Should internal staff require access they would need to follow our admin access process and complete a request form.	Compliant	
A7.6 Use of Accounts How do you ensure that staff only use administrator accounts to carry out administrative activities (such as installing software or making configuration changes)? You must ensure that administrator accounts are only used when absolutely necessary, such as when installing software. Using administrator accounts all-day-long exposes the device to compromise by malware.	We ensure administrator accounts are only given to those who need them to do their job, which includes installing new software and changing configuration settings. We also outline in our security policy that no users who log in as admin should perform any tasks other than administrative duties whilst logged in.	Compliant	
A7.7 Managing Usage How do you ensure that administrator accounts are not used for accessing email or web browsing? 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. You may not need a technical solution to achieve this, it could be based on good policy and procedure as well as regular training for staff.	Our security policy prohibits this. We also set up group policy so that admin accounts on the server cannot be used for web browsing.	Compliant	

Question	Answer	Score	Comments
A7.8 Account Tracking Do you formally track which users have administrator accounts in your organisation? You must track by means of list or formal record all people that have been granted administrator accounts.	Yes Applicant Notes: Yes, we have an admin account register which is reviewed periodically. This is held by IT Desk who are the only ones who have admin access.	Compliant	
A7.9 Access Review Do you review who should have administrative access on a regular basis? You must review the list of people with administrator access regularly. Depending on your business, this might be monthly, quarterly or annually. Any users who no longer need administrative access to carry out their role should have it removed.	Yes Applicant Notes: Yes, the admin account register is reviewed regularly.	Compliant	
A7.10 Two-factor Authentication Have you enabled two-factor authentication for access to all administrative accounts? If your systems supports two factor authentication (where you receive a text message, a one-time code, use a finger-print reader or facial recognition in addition to a password), then you must enable this for administrator accounts.	No	Compliant	
A7.11 Two-factor Unavailable Is this because two-factor authentication is not available for some or all of your devices or systems? List the devices or systems that do not allow two-factor authentication. You are not required to purchase any additional hardware or install additional software in order to meet this requirement. Most standard laptops do not have two-factor authentication available. If your systems do not have two-factor authentication available answer yes to this question.	We use windows computers which done have native 2FA functionality.	Compliant	

Question	Answer	Score	Comments
A8.1 Malware Protection Are all of your computers, laptops, tablets and mobile phones protected from malware by either: A - having anti-malware software installed, B - limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications) or C - application sandboxing (i.e. by using a virtual machine)? 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.	B - Only allowing software from an App Store or Application Whitelisting ,C - Application sandboxing (such as a virtual machine (VM)),A - Anti-Malware Software	Compliant	
A8.2 Update Daily (A) Where you have anti-malware software installed, is it set to update daily and scan files automatically upon access? This is usually the default setting for anti-malware software. You can check these settings in the configuration screen for your anti-virus software. You can use any commonly used anti-virus 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 (A) 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-virus software should have a plugin for your internet browser or for the operating system itself that prevents access to known malicious websites. On Windows 10, SmartScreen can provide this functionality.	Yes	Compliant	

Question	Answer	Score	Comments
A8.4 Application Signing (B) Where you use an app-store or application signing, are users restricted from installing unsigned applications? By default, most mobile phones and tablets restrict you from installing unsigned applications. Usually you have to 'root' or 'jailbreak' a device to allow unsigned applications.	Yes Applicant Notes: We don't allow jailbreaking or rooting so users are unable to install unsigned apps	Compliant	
A8.5 list of Approved Applications (B) 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 document 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, process and training of staff.	Yes Applicant Notes: We have an approved software list which users reference before downloading software	Compliant	
A8.6 Application Sandboxing (C) Where you use application sandboxing, do you ensure that applications within the sandbox are unable to access data stores, sensitive peripherals and your local network? Describe how you achieve this. If you are using a virtual machine to sandbox applications, you can usually set these settings within the configuration options of the virtual machine software.	Sandboxing is performed in an isolated environment which has no access to any external data, peripherals or network	Compliant	
A3.1 Head Office Is your head office domiciled in the UK and is your gross annual turnover less than £20m? This question relates to the eligibility of your company for the included cyber insurance.	Yes	Compliant	

Question	Answer	Score	Comments
A3.2 Cyber Insurance If you have answered 'yes' to the last question then your company is eligible for the included cyber insurance if you gain certification. If you do not want this insurance element please opt out here. The cost of this is included in the assessment package and you can see more about it at [https://www.iasme.co.uk/cyberessentials/automatic-insurance-cover/.](https://www.iasme.co.uk/cyberessentials/automatic-insurance-cover/)	Opt-In	Compliant	
A3.3 Total Gross Revenue What is your total gross revenue? Please provide figure to the nearest £100K. You only need to answer this question if you are taking the insurance. The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification. Please be as accurate as possible - figure should be to the nearest £100K	£3m	Compliant	
A3.4 FCA Is the company or its subsidiaries any of the following: medical, call centre, telemarketing, data processing (outsourcers), internet service provider, telecommunications or an organisation regulated by the FCA? You only need to answer this question if you are taking the insurance. The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.	No	Compliant	
A3.5 Domiciled Operation Does the company have any domiciled operation or derived revenue from the territory or jurisdiction of Canada and / or USA? You only need to answer this question if you are taking the insurance. The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.	No	Compliant	

Question	Answer	Score	Comments
A3.6 Email Contact What is the organisation email contact for the insurance documents? You only need to answer this question if you are taking the insurance. The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification and they will use this to contact you with your insurance documents and renewal information.	accounts@tachart.com	Compliant	
All Answers Approved Have all the answers provided in this assessment been approved at Board level or equivalent?	Yes	Compliant	
Cyber Insurance Declaration Signed Has the attached Cyber Insurance Declaration been downloaded (by clicking here), completed and signed (by a Board level or equivalent signatory), then uploaded (using the function provided below)? Please note: The file upload must be in .PDF, .JPG or .PNG format and a maximum file size of 5MB. If your file is larger than 5 MB, please contact info@iasme.co.uk	Yes Applicant Notes: Insurance PDF attached	Compliant	

CYBER
ESSENTIALS

Certificate of Assurance

TACHART LIMITED

Bnm Building Whitelea Road Swinton
Mexborough
S Yorkshire
S64 8BH
Scope: Whole Company

Complies with the requirements of the Cyber Essentials Scheme

Date of Certification: 18th October 2019
Recertification Due: Oct 2020
Certificate Number: IASME-A-013702
Profile Published: February 2017

CYBER
ESSENTIALS

Certification Body: Netcom Technologies Ltd

Assessor: Shane Hunt

Accreditation Body: IASME Consortium ®

This Certificate certifies that the organisation named was assessed as meeting the Cyber Essentials implementation profile published in February 2017 and thus that, at the time of testing, the organisations ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisations defences will remain satisfactory against cyber attack.