Cyber Essentials Scheme

Report date: 3/11/2026
Applicant: PROTAFORM SPRINGS & PRESSINGS LIMITED,

Validated by: Richard Batchelor, Quality Director

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 (Danzell) scheme. Your certificate number is **d0aba556-f4f2-45b7-ae09-197f45940833** and can be found here:

https://registry.blockmarktech.com/certificates/d0aba556-f4f2-45b7-ae09-197f45940833/

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

Applicant Answers

	Applicant Answers	Assessor Score
Acceptance Please read these terms and conditions carefully. Do you agree to these terms? NOTE: if you do not agree to these terms, your answers will not be assessed or certified.	I accept	Compliant
A1.1 Organisation Name What is your organisation's name?	PROTAFORM SPRINGS & PRESSINGS LIMITED	Compliant
A1.2 Organisation Type What type of organisation are you?	LTD - Limited Company (Ltd or PLC)	Compliant
A1.3 Organisation Size How many employees are there in the organisation?	65, with 17 having access to a device/account.	Compliant
A1.4 Organisation Number What is your organisation's registration number?	01759238	Compliant
A1.5 Registered Address What is your organisation's registered address?	United Kingdom Custom Fields: Applicant Notes: 76 Arthur St Redditch B98 8LJ Address Line 1: 76 Arthur St Address Line 2: Redditch Postcode: B98 8LJ	Compliant
A1.5.1 Operational Address Please provide the operational addresses, if different to your registered address.	76 Arthur St Redditch B98 8LJ	Compliant

A1.6 Legal entities Do you have more than one legal entity, including subsidiaries, within the scope of this assessment?	No	Compliant
A1.7 Organisation Occupation What is your main business?	Manufacturing	Compliant
A1.8 Website Address What is your website address?	https://www.protaform.com	Compliant
A1.9 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?	Renewal	Compliant
A1.10 Reasons for Certification What are the two main reasons for applying for certification?	To Give Confidence to Our Customers Custom Fields: Secondary Reason: Required by Insurer	Compliant
A1.11 CE Requirements Document Have you read the 'Cyber Essentials Requirements for IT Infrastructure' document?	Yes	Compliant
A1.12 Cyber Advisor Have you spoken to an assured NCSC Cyber Advisor to help with your application? Find an assured Cyber Advisor	No	Compliant
A1.13 Cyber Breach Can IASME and their expert partners contact you if you experience a cyber breach?	Yes	Compliant
A1.14 Awareness of Cyber Essentials Where did you hear about Cyber Essentials?	Tender	Compliant
A1.15 Contact Permission Can IASME contact you for research purposes?	No	Compliant

A1.16 Early Warning Have you signed up to the NCSC's free Early Warning service?	Yes	Compliant
A2.1 Assessment Scope Is this assessment for your whole organisation or only a part of it?	Whole organisation	Compliant
A2.3 Network Locations Are the networks included in the scope of this assessment being used at the company locations you provided earlier?	Yes	Compliant
A2.3.1 Site connections Do you have an internet connection for each site in your organisation?	Yes	Compliant
A2.4 Networks Please provide a list of networks that will be in scope for this assessment.	Main Network at Head Office for all operations	Compliant
A2.4.1 Home or remote workers How many staff are home or remote workers?	6	Compliant
A2.4.2 Home/remote worker connection How are home/remote workers connecting to your organisational data and services?	Corporate VPN	Compliant
A2.5 Network Equipment Please provide a list of network equipment that will be in scope for this assessment (including firewalls and routers). You must include make, model and quantity of each device listed.	1 x pfSense Firewall (VM) v2.8.2 Windows laptops, and desktops servers feature the Windows Firewall which is used on all such devices.	Compliant

A2.6 End User Devices Please list the quantities and operating systems for your laptops, desktops and virtual desktops within the scope of this assessment. Please Note: You must include make and operating system versions for all devices. All user devices declared within the scope of the certification only require the make and operating system to be listed. We have removed the requirement for you to list the model of the device. Only in-scope devices connecting to cloud services must be included in the assessment. Devices outside the declared scope are excluded, but user accounts accessing the cloud service must comply with Cyber Essentials controls, including mandatory MFA. A scope that does not include end user devices is not acceptable.	2 Lenovo Laptops running Windows 11 Pro 25H2 1 Dell Laptop running Windows 11 Pro 25H2 1 Lenovo PC running Windows 11 Pro 25H2 1 VM running Windows Server Standard 2019 1809 (RDS Session Server)	Compliant
A2.6.1 Thin Client Devices Please list the quantity of thin clients within the scope of this assessment. Please include make and operating systems.	10 HP Thin Pro 8.1 devices restricted to RDP only. 1 HP Thin Pro 8.1 device restricted to a single webpage.	Compliant
A2.7 Server Devices Please list the quantity of servers, virtual servers, virtual server hosts (hypervisors) and Virtual Desktop Infrastructure (VDI) servers. You must include the operating system.	1 HP HyperV Server running Windows Server Standard 2019 1809 4 VMs running Windows Server Standard 2019 1809	Compliant
A2.8 Mobile Devices Please list the quantities of tablets and mobile devices within the scope of this assessment.	4 x Samsung mobiles Android OS 16, 1 x Apple iPhone iOS 26, 35 Lenovo Tablets Android OS 17.	Compliant
A2.9 Cloud Services Please list all the cloud services that are in use by your organisation and provided by a third party. Please note that cloud services cannot be excluded from the scope of Cyber Essentials.	Matics Microsoft 365 Apple and Google services are not used.	Compliant

A2.10 Responsible Person Please provide the name and role of the person who is responsible for managing your IT systems in the scope of this assessment.	Des Fagg Custom Fields: Responsible Person Role: Managing Director	Compliant
A3.1 Head Office Is your head office domiciled in the UK or Crown Dependencies and is your gross annual turnover less than £20m?	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. Would you like to opt in for the included cyber 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?	Yes	Compliant
A4.1.1 Off Network Firewalls Do you have software firewalls enabled on all of your computers, laptops and servers?	Yes	Compliant
A4.2 Firewall Default Password When you first receive an internet router or hardware firewall device, it may have had a default password on it. Have you changed all the default passwords on your boundary firewall devices?	Yes	Compliant
A4.2.1 Firewall Password Change Process Please describe the process for changing your firewall password. Home routers not supplied by your organisation are not included in this requirement.	The firewall password is changed by logging on to a web-based GUI from within the internal network, selecting users, select the admin account, change the password and save. On Windows devices, the machines are enrolled in EntraID using an existing admin account, and user is added as a non-admin accounts. All Windows-based machines are Windows 11 based; therefore, the Local administrator account is disabled by default by Microsoft. This is left unchanged.	Compliant

A4.3 Firewall Password Configuration How is your firewall password configured? Please select the option being used: A. Multi-factor authentication, with a minimum password length 8 characters and no maximum length B. Automatic blocking of common passwords, with a minimum password length 8 characters and no maximum length C. A password minimum length of 12 characters and no maximum length D. Passwordless system is being used as an alternative to user name and password, please describe E. None of the above, please describe	0: C. A password minimum length of 12 characters and no maximum length Custom Fields: Applicant Notes: The firewall GUI can only be accessed from the internal network. Passwords are a minimum of 30 characters and meet complexity requirements.	Compliant
A4.4 Firewall Password Issue Do you change your firewall password when you know or suspect it has been compromised?	Yes	Compliant
A4.5 Firewall Management Process Do you have a process to manage your firewall?	Yes Custom Fields: Applicant Notes: Any changes have to be approved at board level and documented, along with periodic review to ensure requirements.	Compliant
A4.6 Firewall Review Process Have you reviewed your firewall rules in the last 12 months? Please describe your review process.	Yes, we do not have open ports other than the VPN, which is required for business. If we had such requirements; The IT team carries out a monthly review of all services, rules and policies on the firewall. They would be checked at the board level for removal. This would also be confirmed to the board on completion. Currently, an annual check is carried out on the pfSense firewall.	Compliant
A4.7 Firewall Inbound Connections Is your firewall configured to allow unauthenticated inbound connections?	No	Compliant
A4.8 Allowed Connections Please describe how you approve and document your allowed inbound connections.	We have a single VPN service, which is required for business. If we had any other such requirements, they would be recorded in the IT change log and approved at the board level.	Compliant

A4.9 Firewall Remote Configuration Are your boundary firewalls configured to allow access to their configuration settings over the internet?	No	Compliant
A5.1 Remove Unused Software Have you removed or disabled software and services that you do not use on your laptops, desktop computers, thin clients, servers, tablets, mobile phones and cloud services? Describe how you achieve this.	All non-essential software is removed from new devices manually during setup. All devices are monitored and non-approved applications are flagged for review if found (in case an application is missed during manual setup, users do not have rights to install software). Application provisioning via the Microsoft 365 tenant is limited to required applications for the user, and functionality is limited by user accounts, such as Teams groups.	Compliant
A5.2 Remove Unnecessary 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?	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?	Yes Custom Fields: Applicant Notes: Passwords are 30 chars minimum and meet complexity requirements; these are generated to be unique.	Compliant
A5.4 Internally Hosted External Services Do you run or host external services that provide access to data (that shouldn't be made public) to users across the internet?	Yes	Compliant

A5.5 External Services Authentication Option If yes to question A5.4, which authentication option do you use? A. Multi-factor authentication, with a minimum password length of 8 characters and no maximum length B. Automatic blocking of common passwords, with a minimum password length of 8 characters and no maximum length C. A minimum password length of 12 characters and no maximum length D. Passwordless, please describe E. None of the above, please describe	0: A. Multi-factor authentication, with a minimum password length of 8 characters and no maximum length, 1: B. Automatic blocking of common passwords, with a minimum password length of 8 characters and no maximum length, 2: C. A minimum password length of 12 characters and no maximum length	Compliant
A5.6 External Services Password Change Describe the process in place for changing passwords on your external services when you believe they have been compromised.	In any notification of a possible compromise, passwords would be changed. The firewall password is changed by logging on to a web-based GUI from within the internal network, selecting users, select the account, change the password, generate a new user certificate and save. The new certificate and password would then be used with the device after the device has been deemed safe.	Compliant
A5.7 Brute Force Protection When not using multi-factor authentication, which option are you using to protect your external service from brute force attacks? A. Throttling the rate of attempts B. Locking accounts after no more than 10 unsuccessful attempts C. None of the above, please describe	0: A. Throttling the rate of attempts, 1: B. Locking accounts after 10 unsuccessful attempts Custom Fields: Applicant Notes: The use of user certificates further restricts brute force.	Compliant
A5.8 Automatic File Execution Have you disabled any feature which allows automatic file execution of downloaded or imported files without user authorisation?	Yes Custom Fields: Applicant Notes: Automatic file execution is disabled across all devices, except where this is part of an automated update system for existing applications.	Compliant
A5.9 Device Unlocking When a device requires a user to have the device in hand, do you set a locking mechanism on your devices to access the software and services installed?	Yes	Compliant

A5.10 Device Unlocking Method Which method do you use to unlock the devices?	All devices require a pin/password of 6 or more characters and will lock out further attempts, requiring admin intervention after 5 failed attempts.	Compliant
A6.1 Supported Operating System Are all operating systems on your devices supported by a vendor that produces regular security updates and vulnerability fixes? If you have included firewall or router devices in your scope, the firmware of these devices is considered to be an operating system and needs to meet this requirement.	Yes	Compliant
A6.2 Supported Software Is all the software on your devices supported by a supplier that produces regular vulnerability fixes for any security problems?	Yes	Compliant
A6.2.1 Internet Browsers Please list all internet browser(s) installed on your device. The version is required.	Google Chrome 153 Edge Version 152 Safari Version 27	Compliant Assessor Notes: Supported at time of marking. Applicant confirmed now updated to latest versions
A6.2.2 Malware Protection Please list your malware protection software. The version is required.	Webroot/Opentext Core Endpoint 9.0.45.50	Compliant
A6.2.3 Email Applications Please list all your email applications installed on end user devices and servers. The version is required.	Office 365 E3 - Outlook for 365 (2608)	Compliant
A6.2.4 Office Applications Please list all office applications that are used to create organisational data. The version is required.	Office 365 E3	Compliant
A6.3 Software Licensing Are any of the in-scope software or cloud services unlicensed or unsupported?	No	Compliant

A6.4 Security Updates - Operating System Are all high-risk or critical security updates and vulnerability fixes for operating systems and router and firewall firmware installed within 14 days of release?	Yes	Compliant
A6.4.1 Auto-updates - Operating System Are all updates applied for operating systems by enabling auto updates?	Yes	Compliant
A6.5 Security Updates - Software Are all high-risk or critical security updates and vulnerability fixes for software (including any associated files and extensions) installed within 14 days of release?	Yes	Compliant
A6.5.1 Auto-updates - Software Are all updates applied on your software by enabling auto updates?	Yes	Compliant
A6.6 Unsupported Software Removal Have you removed any software installed on your devices that is no longer supported and no longer receives regular updates or vulnerability fixes for security problems?	Yes Custom Fields: Applicant Notes: Any software that is no longer required or is out of support is removed at expiry.	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.	No unsupported software is used across the organisation.	Compliant
A7.1 User Account Creation Are your users only provided with user accounts after a process has been followed to approve their creation? Describe the process.	All accounts (regardless of platform) are requested at the board level with the specific requirements, changes or removals are also provided by a board member.	Compliant
A7.2 Unique Credentials Are all your user and administrative accounts accessed by entering unique credentials?	Yes	Compliant

A7.3 Leaver Accounts How do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation?	A users accounts are disabled to preserve auditing information during the staff exit procedure carried out with the staff member exiting, or immediately in the case of instant dismissal or investigation. The return of any devices and removal of VPN account if provided is completed at the same time.	Compliant
A7.4 User Privileges Do you ensure that staff only have the access privileges that they need to do their current job? How do you do this?	Staff are only provided permissions to access data on any platform specifically required for their role. If a role changes, the permissions are changed in line with the new role at the change of role. The assignment of roles and changes are approved at board level, and permissions are role-based.	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?	The assignment of admin roles and changes must be approved at board level. Admin accounts are provided for the administration of systems only and are not used for general work tasks.	Compliant
A7.6 Use of Administrator Accounts How does your organisation make sure that separate accounts are used to carry out administrative tasks (such as installing software or making configuration changes)? This applies to local administrator accounts, network/domain administrator accounts, and cloud service administrator accounts.	Admin level accounts are provided for the administration of systems only and are not used for general work tasks. This applies across all devices and services. This is restricted by company policy and the provision of Administrator accounts is only made to support staff that do not operate systems as Users.	Compliant
A7.7 Managing Administrator Account Usage How does your organisation prevent administrator accounts from being used to carry out everyday tasks like browsing the web or accessing email?	This is restricted by company policy and the provision of Administrator accounts is only made to support staff that do not operate systems as end users. Company policy and procedures require web browsing and email access to be restricted to standard user accounts only. All staff are required to sign the policy and are reminded annually.	Compliant
A7.8 Administrator Account Tracking Do you formally track which users have administrator accounts in your organisation?	Yes Custom Fields: Applicant Notes: Accounts are approved and tracked at board level.	Compliant
A7.9 Administrator Access Review Do you review who should have administrative access on a regular basis?	Yes	Compliant

A7.10 Brute Force Protection Where you have systems that require passwords (or where passwords are a backup for a passwordless system), how are they protected from brute-force attacks?	Accounts are locked out after 5 attempts, and IT support is automatically notified. Locked accounts are only unlocked if a review of the reason is deemed non-malicious.	Compliant
A7.11 Password Quality Which technical controls are used to manage the quality of your passwords within your organisation?	Minimum length enforcement of 12 characters. Password must not contain the users account name or more than two consecutive characters from the users full name. Password must contain characters from three of the following four categories: Uppercase characters A-Z (Latin alphabet) Lowercase characters a-z (Latin alphabet) Digits 0-9 Special characters (!, $, #, %, etc.) MFA where available Users are guided to use a sentence or string of words.	Compliant
A7.12 Password Creation Advice Please explain how you encourage people to use unique and strong passwords.	Users are guided to use a sentence or string of words. We do not enforce password expiry but do enforce complexity. User services are SSO with one additional account, so they only have to remember a couple of passwords which they use daily.	Compliant
A7.13 Password Compromise Policy Do you have a process for when you believe the passwords or accounts have been compromised?	Yes Custom Fields: Applicant Notes: Any indication of a compromised account will lead to the account being disabled and reviewed for the cause of the leak and future countermeasures. Once any risk has been mitigated, the password is changed, and the account is reenabled.	Compliant
A7.14 Cloud Service MFA Do all of your cloud services have multi-factor authentication (MFA) available as part of the service? A cloud service is an on-demand, scalable service, hosted on shared infrastructure, and accessible via the internet. For the purposes of Cyber Essentials a cloud service will be accessed via an account (which may be credentials issued by your organisation, or an email address used for business purposes) and will store or process data for your organisation.	Yes	Compliant

A7.16 Administrator MFA Has MFA been applied to all administrators of your cloud services, excluding any listed in A7.15 that do not provide it?	Yes	Compliant
A7.17 User MFA Has MFA been applied to all users of your cloud services, excluding any listed in A7.15 that do not provide it?	Yes	Compliant
A8.1 Malware Protection Are all of your desktop computers, laptops, tablets and mobile phones protected from malware by either: A - Having anti-malware software installed and/or B - Limiting installation of applications by application allow listing - for example, using an app store and a list of approved applications, using a Mobile Device Management (MDM) solution or C - None of the above, please describe	0: A - anti-malware software, 1: B - limiting installation of applications by application allow listing from an approved app store Custom Fields: Applicant Notes: Webroot Endpoint Protection along with ManageEngine MDM.	Compliant
A8.2 Anti-Malware Updates If Option A has been selected: Where you have anti-malware software installed, is it set to update in line with the vendor's guidelines and prevent malware from running on detection?	Yes Custom Fields: Applicant Notes: Cloud based scanning will remove threats before they can be executed.	Compliant
A8.3 Scanning Web Pages If Option A has been selected: Where you have anti-malware software installed, is it set to scan web pages you visit and warn you about accessing malicious websites?	Yes Custom Fields: Applicant Notes: Webroot plugin within browsers blocks malicious or suspicious websites.	Compliant
A8.4 Application Signing If Option B has been selected: Where you use an app-store or application signing, are users restricted from installing unsigned applications?	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?	Yes Custom Fields: Applicant Notes: Managed by MDM.	Compliant
Attestation 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