

Cyber Essentials Scheme

Report date: 9/9/2026
Applicant: Midland Bright Steels Ltd,

Validation Attached

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 **a4d98df3-572e-432b-b421-71b2605da5a5** and can be found here:

<https://registry.blockmarktech.com/certificates/a4d98df3-572e-432b-b421-71b2605da5a5/>

Your insurance number is 0038326543 and it can be found here:

<https://registry.blockmarktech.com/certificates/618a2ca4-43f4-4cc0-91af-d785642a82b2/>

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

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

Applicant Answers

	Applicant Answers	Assessor Score
Acceptance Please read these terms and conditions carefully. Do you agree to these terms? NOTE: if you do not agree to these terms, your answers will not be assessed or certified.	I accept	Compliant
A1.1 Organisation Name What is your organisation's name?	MIDLAND BRIGHT STEELS 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?	5-9 EMPLOYEES	Compliant
A1.4 Organisation Number What is your organisation's registration number?	03970194	Compliant
A1.5 Registered Address What is your organisation's registered address?	United Kingdom Custom Fields: Postcode: DY5 3EE County: West Midlands Town/City: Brierley Hill Address Line 1: Swinford House Albion Street	Compliant
A1.5.1 Operational Address Please provide the operational addresses, if different to your registered address.	Inverclyde Drive Off, Birmingham New Rd, Wolverhampton WV4 6FB	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?	Other (please describe) Custom Fields: Applicant Notes: Steel Stockholding	Compliant
A1.8 Website Address What is your website address?	midlandbrightsteels.co.uk	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?	First Time Application	Compliant
A1.10 Reasons for Certification What are the two main reasons for applying for certification?	To Generally Improve Our Security Custom Fields: Secondary Reason: To Give Confidence to Our Customers	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?	Cyber Advisor	Compliant
A1.15 Contact Permission Can IASME contact you for research purposes?	Yes	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?	All in-scope networks are being used at company location listed in A1.5.1 (Midland Bright Steels Ltd. Inverclyde Drive(off Birmingham New Road),Wolverhampton, WV4 6FB)	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 - used for all staff and services. Home worker network - used for all remote / home workers Remote network for sister company - site to site VPN for sister company - devices from sister network connect into an RDS server hosted on the main network.	Compliant
A2.4.1 Home or remote workers How many staff are home or remote workers?	5	Compliant
A2.4.2 Home/remote worker connection How are home/remote workers connecting to your organisational data and services?	Home / remote workers connect VIA a corporate VPN. This VPN connection is secured using a 12 character password with no maximum length requirement.	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 Cisco 1117-4P router 1 x SONICWALL SOHO 250W Home / remote users are protected by the built in firewall included with Bitdefender Gravityzone. All organisational devices are protected by Bitdefender GravityZone Endpoint Security. The Bitdefender software firewall is enabled on all company managed devices and configured to block unsolicited inbound connections. Local administrator passwords are managed by the MSP only. Where a password change is required, the change is performed by the MSP using their RMM. Access to local administrator accounts is restricted to MSP personnel only, and all changes are logged. Standard users do not have local administrator privileges. The MSP will change the administrator password if required via the RMM and log out and back in to that account to ensure the password is updated. Azure Global Administrator accounts are restricted to MSP only. Any change to Global Administrator credentials requires approval from a director and is performed by an existing Global Administrator. MFA is enforced on all privileged accounts. Password changes are completed through Microsoft Entra , and access is reviewed regularly. When a password change is required for a Microsoft or Azure account the MSP will log in, update the password using a secure password generator and log back in to test the new password.	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.	4 x HP laptops running Windows 11 Professional V25H2 8 x HP desktop PCs running Windows 11 Professional V25H2 1 x Lenovo desktop PC running Windows 11 Professional V25H2	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.	None	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 x physical HP server running Windows Server 2025 Standard v24H2 1 x physical HP server running Windows Server 2019 Standard v1809	Compliant Assessor Notes: Specify if the servers are physical or virtual, and for virtual servers, provide details of their hosting environment. eg Hyper-V, ESXi(version needed), AWS, Azure etc
A2.8 Mobile Devices Please list the quantities of tablets and mobile devices within the scope of this assessment.	6 x Apple iPhone iOS v26.6.1	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.	MS 365 8x8 Bitdefender Gravityzone (Managed by MSP) NinjaOne (Managed by MSP) HSBC	Compliant Assessor Notes: The following cloud services were mentioned elsewhere in the assessment but are not listed in A2.9: Bitdefender Gravityzone, NinjaOne RMM and password manager (as referenced in the assessment).
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.	Stephen Sutton Custom Fields: Responsible Person Role: 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-In	Compliant
A3.3 Insurance Contact What is the organisation email contact for the insurance documents? You only need to answer this question if you are taking the insurance.	s.sutton@midlandbrightsteels.co.uk	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.	When changing the firewall password an engineer from our MSP, will log in to the firewall and change the password from the default password to a secure password auto generated by a random password generator, ensuring the password consists of at least 12 characters consisting of lower/uppercase , numbers and a symbol(s)with no maxium length requirements. The engineer will then log out of the firewall and attempt to log in with the old and new password to ensure the password has successfully changed. For any home or remote workers, the administrator password of the local device will be changed by our MSP. This is done remotely using their RMM and will be changed using a secure password generator such as lastpass. Once the password has been updated the MSP will log into the device using the new password confirming update is successful.	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	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	Compliant
A4.6 Firewall Review Process Have you reviewed your firewall rules in the last 12 months? Please describe your review process.	Any services open on the firewall are audited annually and if no longer required our MSP will be informed and action the deactivation of these services to ensure any services which arent required have been made secure. Our MSP will review the open services as part of there documented processes and inform a director or a person responsible for the IT services. The decision will then be made by a director as to whether these services are required for the business or not. If services are no longer required our MSP will be informed and disable the services,they will then perform checks to ensure the services cannot be accessed.	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.	Any required inbound connections are to only be enabled if approved by a director of the company. Once approved the requirement and business need will be documented in the company handbook. These services will be reviewed annually to review the risks and if they are still required for the business, if not, they will be immediately disabled by the MSP.	Compliant
A4.9 Firewall Remote Configuration Are your boundary firewalls configured to allow access to their configuration settings over the internet?	Yes	Compliant
A4.10 Business Need for Access If you answered yes in question A4.9, is there a documented business requirement for this access?	Yes	Compliant
A4.11 Firewall Settings Protection If you answered yes in question A4.9, 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?	MFA is enabled for the MSP to access NinjaOne RMM and Bitdefender Gravityzone portal, which controls the software firewalls. Physical onsite firewall (Sonicwall) cannot be accessed over the internet, all HTTP/S connections are blocked.	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 company devices are built and setup with a standard build, the build only contains applications, system utilities and network services which are required for day-to-day use of the company all other software / applications are uninstalled. Any software which maybe installed post deployment is also monitored by our MSP IT monitoring software (Ninja RMM), from this the software can be reviewed and removed if required. All users are also fully restricted from installing any software, therefore software cannot be installed without domain administrator permissions which is fully controlled by our MSP. Any software that is requested to be installed must be on the approved software list or approved by a director. Any cloud services that are not used or required for the organisation will be disabled or removed as part of the onboarding these will be reviewed and approved by a director of the company.	Compliant Assessor Notes: Please also confirm how unused software, services and accounts are reviewed and removed across your cloud services, as well as on your devices.

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	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: 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.	If any external service such as VPN accounts are suspected to have a compromised password, the end users are advised to immediately contact our IT MSP and report the breach. Our IT MSP will then immediately change the password and check for any unusual logins. Our IT also monitor for any unusual logins using the SonicWall firewall and action on any suspicious activity.	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: B. Locking accounts after 10 unsuccessful attempts	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	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?	To unlock devices the users are required to enter a password of 12 characters, with no maximum length requirements. This password must comply with the full password requirements and will be locked out after 5 or more incorrect attempts. All mobile phones have biometric or passcode access enabled, therefore to access the device the user would have to use their fingerprint/face recognition to unlock the phone or a 6 digit code without biometric. When unlocking a device with a pin code this will only unlock the device and does not provide access to any organisational data and services without further authentication.	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 v152.0.7977.83 Microsoft Edge v152.0.4191.66 Safari v26	Compliant
A6.2.2 Malware Protection Please list your malware protection software. The version is required.	Bitdefender Endpoint Security 8.26.9.664	Compliant
A6.2.3 Email Applications Please list all your email applications installed on end user devices and servers. The version is required.	Outlook MS365, Apple Mail v26	Compliant
A6.2.4 Office Applications Please list all office applications that are used to create organisational data. The version is required.	MS 365	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	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.	Organisation does not use any unsupported software. This has been audited by our MSP using their RMM platform which reports on any software which no longer receives software updates. All software installed on devices within organisation currently receives security updates.	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 requests for new users are processed by MSP. They are instructed to only accept requests from a director of the organisation.	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?	When an employee leaves the organisation, a director will inform the MSP who will ensure all accounts are disabled and access from all systems revoked on the last day of employment.	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?	Employees are only given access to the resources needed to do their day to day job, these permissions are agreed with the director of the company. If an employee requires their permissions amending the director will make a request to the MSP who will amend the access accordingly. Should an employee change roles within the company a request will be submitted to the director who will approve and request from MSP to grant / amend existing access.	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?	Administrative access is only given at the request of a director. Once approved a separate administrator account is created by our MSP with a unique password generated using a secure password generator.	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.	All administrative accounts are separate to accounts used for day to day work and have separate passwords associated to the main users account.	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?	Administrative accounts, including those used by our MSP, are separate from standard user accounts and are only used for administrative activities requiring elevated privileges. Administrative accounts are not used for routine tasks such as email, web browsing, editing files. Users and MSP engineers use standard user accounts for day-to-day activities and only use administrative accounts when performing authorised administrative tasks. This is enforced through company policy, user awareness, and the use of separate administrative credentials for privileged access. Where administrative access is required, it is used only for the duration of the task being performed.	Compliant
A7.8 Administrator Account Tracking Do you formally track which users have administrator accounts in your organisation?	Yes	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?	Computer accounts are protected from brute-force guessing by blocking the accounts after 5 consecutive incorrect attempts. All cloud accounts are also protected by multi factor authentication. iPhones are protected from brute-force attacks through Apples built-in passcode protection mechanisms. Devices require a strong passcode and automatically enforce increasing time delays after repeated failed authentication attempts, preventing rapid password guessing. Device data is encrypted and access is restricted until the correct passcode is entered.	Compliant
A7.11 Password Quality Which technical controls are used to manage the quality of your passwords within your organisation?	All cloud accounts are protected by multi factor authentication. The passwords must consist of a minimum of 8 characters with no maximum length requirements. We also enforce a group policy which enforces account security controls such as minimum password length to 12 characters with no maximum length restrictions, passwords must meet complexity requirements,. User accounts are protected by an account lockout policy after multiple failed login attempts.	Compliant
A7.12 Password Creation Advice Please explain how you encourage people to use unique and strong passwords.	Staff are encouraged to use a secure password generator when creating new passwords. Use of strong passwords and requirements are also listed in the IT policy, along with regular advice from our MSP and NCSCs guidance.	Compliant
A7.13 Password Compromise Policy Do you have a process for when you believe the passwords or accounts have been compromised?	Yes	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	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	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	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	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