G-Cloud 15 Service Definition Document

Cyber Essentials,
Cyber Essentials Plus,
Defence Cyber Certification,
CyberSmart Core and CyberSmart Complete

v15.2

Who is CyberSmart?

Our Vision

A world where millions of organisations trust CyberSmart to help them combat the constant threat of cyber-attacks and increasing regulation in an ever-evolving technological landscape and increasingly connected digital operating space. CyberSmart will be the automated compliance and assurance team for businesses. An agile platform, CyberSmart just gets the job done, allowing businesses to concentrate on growing.

Who we are

Born out of a GCHQ accelerator in 2017, CyberSmart was created by a group of forward-thinking security experts, who noticed that many companies needed to secure themselves and achieve information security standards, but ultimately found the process too complicated or were limited by financial or human resources.

The team believes that every organisation should be able to easily comply with recognised standards and protect their data and infrastructure. Through making security accessible, they have achieved tremendous growth and protect tens of thousands of users.

What Services can CyberSmart provide to support your organisation?

Our services:

- Cyber Essentials certification:
    - Cyber Essentials is an official UK wide, government-backed certification scheme that helps companies guard against the most common cyber threats and reduce their risks by at least 80%.
    - The scheme also allows organisations to demonstrate their commitment to cyber security to their customers.
    - To achieve Cyber Essentials certification, an organisation must complete a self-assessment questionnaire and certify they have the five technical controls in place in their organisation.
    - Using CyberSmart's services, an organisation can achieve same-day certification, with our smart questionnaire and automated device compliance software (CyberSmart Active Protect).
    - CyberSmart delivers rapid, online certification services to achieve Cyber Essentials certification.
    - Using our bespoke, secure cloud based portal we enable organisations to complete the self-assessment question set without recourse to expensive or qualified technical assistance.
    - Guided responses embedded into the platform clarify technical questions.
    - Our software and internal auditing team combine to review all applications and flag back to organisations any questions requiring additional detail or clarification prior to submission for certification.
    - As an official Certification Body under the Cyber Essentials Scheme, CyberSmart is authorised to submit applications on behalf or organisations to achieve their certificate. Certificates are available to download by the organisation immediately after certification.
    - The CyberSmart platform enables a one stop, end-to-end solution to achieve Cyber Essentials certification.
    - Once an organisation has achieved their Cyber Essentials certification they can elect to pursue, within 3 months, the award of the Cyber Essentials Plus Certificate, which requires a scheduled audit.
- Cyber Essentials Plus certification:
    - Cyber Essentials Plus is the highest level of certification offered under the Cyber Essentials scheme, an official UK wide, government-backed certification that helps companies guard against the most common cyber threats and reduce risk by at least 80%.

- Cyber Essentials Plus ensures organisations have the five technical controls needed in place, with verification requirements prior to certification awarded by a qualified Cyber Essentials Plus auditor.
- We will provide you with a step by step checklist prior to the audit to ensure that you meet the requirements for certification.
- The organisation can choose either a remote or on-site audit which is performed by one of our qualified auditors who supply a written report that highlights any final issues, and will guide the organisation to achieve the standard required for certification.
- When the organisation has completed the compulsory questionnaire and CyberSmart's auditor is satisfied the technical audit has met the necessary standard, we will submit your application and your certificate will typically be issued on the same day.
- The technical audit must be completed within 3 months of completing the Cyber Essentials certification. It requires our CyberSmart qualified auditor to select a representative sample of devices from the organisation to audit to demonstrate technical compliance.
- The cost for Cyber Essentials Plus certification is a variable cost, dependant upon a number of factors such as, but not limited to:
  - The number of devices within the organisation
  - The number of sites the organisation covers
  - Whether the organisation requires an on-site or remote access audit

- Defence Cyber Certification:
  - Defence Cyber Certification (DCC) is a UK defence supply chain cyber security certification scheme aligned to the Ministry of Defence Cyber Security Model (CSMv4).
  - CyberSmart is authorised to assess and certify organisations for Defence Cyber Certification at Level 0 and Level 1.
  - CyberSmart acts as the Certification Body for the purposes of assessment and certification under the Defence Cyber Certification scheme.
  - Defence Cyber Certification may be purchased as a standalone certification or as part of a package with Cyber Essentials certification or CyberSmart Core.
    - CyberSmart Defence Core Packages include Cyber Essentials certification, CyberSmart Active Protect and a set of DCC-ready policy templates.
  - CyberSmart provides guidance documentation, a Body of Evidence pack and supporting policy templates to help organisations prepare for the DCC assessment and submit evidence in line with scheme requirements.
  - Defence Cyber Certification is not currently delivered through the CyberSmart Platform.
    - For DCC Level 0 only, organisations are provided with access to the IASME DCC dashboard to upload evidence as required by the scheme. The availability and operation of the IASME dashboard is the responsibility of IASME.
    - For DCC Level 1, CyberSmart and the applicant will mutually agree on a secure mechanism for the sharing of assessment evidence. The applicant must retain all required evidence for the duration specified by the scheme.
  - Defence Cyber Certification is issued on a three-year certification term. Fees include the cost of one assessment per certification term.
  - As part of the scheme requirements, at Level 0 and Level 1, organisations must hold and maintain Cyber Essentials certification on an annual basis for the duration of their Defence Cyber Certification.
  - If certification is not achieved following an assessment, additional fees may apply for any re-assessment, re-audit or further assessment activity required to achieve certification.
- CyberSmart Platform:

- The CyberSmart Platform performs the following functions:
  - 24/7/365 compliance monitoring for organisation desktop and mobile devices to maintain Cyber Essentials and Cyber Essentials Plus certification requirements
- The Platform consists of two key elements:
  - CyberSmart Active Protect: Desktop and Mobile device applications
    - The CyberSmart app is easily deployed and allows you to get insights into the current security status of all your devices.
    - Organisations can install the CyberSmart software on up to 5 devices per user.
    - CyberSmart supports unlimited users within organisations.
    - The application performs the following checks:
      - macOS:
        - Automatic OS updating enabled
        - Automatic app updates enabled
        - Firewall enabled
        - Stealth mode enabled
        - System Integrity Protection enabled
        - GateKeeper enabled
        - Password enabled
        - Anti-malware installed
        - Current User is a non-admin account
        - Operating System supported
        - Native Full Disk Encryption enabled
      - Microsoft Windows:
        - Automatic OS updating enabled
        - Password enabled
        - Firewall enabled
        - Anti-malware installed
        - Autoplay disabled
        - Current User is a non-admin account
        - Operating System supported
        - Native Full Disk Encryption enabled
      - iOS:
        - Device Rooting check
        - Unlock Authentication check
        - Supported Operating System check
        - Supported Device check
        - Web Protection check
      - Android:
        - Device Rooting check

- Unlock Authentication check
- WiFi Protection check
- Android Debug Bridge check
- App Security check
- Security Patches check
- Google Play Protect check
- Supported Operating System check

- The CyberSmart Active Protect continues to ensure users and their devices remain compliant with checks every 15 minutes.
- Across all operating systems, users can access Smart Policies:
    - Smart Policies are security and compliance policies you upload and distribute from the CyberSmart dashboard to Active Protect.
    - Users see them on their device, read and agree, and acknowledgements are tracked centrally for audit and reporting.
    - You can add, update or remove policies and assign them to specific user groups as needs change.

- CyberSmart administrative portal
    - The cloud-based dashboard is used to manage compliance throughout your organisation.
    - Organisation Admins can add new team members, check the compliance status of individual devices and fix issues within the dashboard.
    - Access to how-to articles and step-by-step instructions ensure that anyone, regardless of technical or compliance knowledge, can use the platform.
    - Access to clear, guided remediation and live support
    - Weekly reporting detailing the status of your organisation and highlighting things the organisation should be aware of.

- Additional modules are included with CyberSmart Core and Complete:
    - CyberSmart Patch (included with both CyberSmart Core and CyberSmart Complete)
        - Helps reduce vulnerabilities by keeping third-party software up to date on Windows and Mac devices with minimal disruption.
        - Provides complete visibility and control over software updates, showing what has been patched, where and when from the CyberSmart dashboard.
        - Supports hundreds of commonly used third-party applications, including browsers, messaging tools and productivity software.
        - Allows updates to be deployed to single devices, groups of devices or entire fleets to maintain consistent software hygiene.
        - Setup is simple and managed from a single dashboard with no extra tools required, with end-user disruption kept to a minimum.
    - CyberSmart Learn Lite (including with CyberSmart Core)
        - The built-in cybersecurity awareness training included with Active Protect, delivering simple, bite-sized learning to help users understand common threats and adopt safer behaviour.
        - The same simple, easy-to-implement training solution formerly known as CyberSmart Academy.

- Training content is accessible online through the CyberSmart platform with minimal setup and no additional licences required.
- Supports organisations in reinforcing basic cyber awareness and improving recognition of common threat types.

- CyberSmart Learn (included with CyberSmart Complete)
  - A fully customisable and scalable security awareness training and learning management system designed for businesses of all sizes.
  - Provides a broad library of pre-built content covering common threats, best practice, compliance topics and broader skills areas.
  - Allows organisations to upload and tailor custom training content using SCORM, PDFs, embedded materials or learner tasks.
  - Provides advanced reporting and real-time progress tracking to monitor cyber awareness and training completion across the business.
  - Integrates with CyberSmart Active Protect or can be used as a standalone platform.
  - Supports phishing simulation via CyberSmart Phish to test user behaviour and reinforce learning with real-world scenarios.
  - Designed for quick deployment, allowing employees to access assigned training using single sign-on or login credentials.

Data Security

- Web Security:
  - We utilise the most secure and resilient stack from AWS which ensures servers are always patched and up to date.
  - Web servers store no sensitive information - this is retrieved from an AES-256 encrypted database accessible only within the virtual private cloud.
  - Automated security tests are performed internally across the code base on every commit.
  - In addition, we undertake regular third party security audits including web application penetration tests to ensure comprehensive coverage.
- Storing passwords securely
  - All passwords are salted and hashed using PBKDF2 with 1.5m iterations using HMAC-SHA256 as the pseudo-random function.
- G Suite / Office 365 authentication
  - We utilise OAuth 2.0 to integrate with these platforms. We do not process or store the users credentials, instead we are provided with a token from the provider which we use to authenticate the user.
- Multi-factor authentication
  - We recommend all users utilise the multi-factor authentication functionality offered in the application.
  - This can be required for an organisation within the settings.
- Internal Security:
  - We are continuously reviewing the effectiveness of our Information Security Management System and are ISO 27001:2022 certified.
  - We undertake regular third party security audits and third party penetration testing. This comes from the understanding that external perspectives are invaluable in securing against modern threats.

    - All staff have had references verified and background checks conducted. Security training is provided to ensure everyone stays on top of their game.
    - All desktop and laptop devices are provisioned under Mobile Device Management (MDM) which allows us to ensure mandated security measures are in place including full disk encryption as well as remote tracking and wiping of lost or stolen devices.
    - We deploy all suitable measures to protect our office network including but not limited to: whitelist only firewalls, segmented VLAN's and a company VPN.
- Data backup and recovery
    - Platform data is stored in the following AWS regions:
        - Primary - London (eu-west-2)
        - Secondary - Ireland (eu-west-1)
    - We utilise multiple availability zones (AZ's) within each region with a secondary failover region to ensure maximum reliability.
    - The exception to this is Cyber Essentials Data, which is only stored within the UK.
    - All stored data is server side encrypted with AES-256.
- Disaster recovery
    - CyberSmart maintains and has achieved and maintains the following accredited certification standards:
        - Cyber Essentials
        - Cyber Essentials Plus
        - IASME Cyber Baseline Level 1
        - IASME Cyber Assurance Level 1
        - IASME Cyber Assurance Level 2, and Quality Principles
        - IASME Quality Principles
        - Defence Cyber Certification Level 0
        - Defence Cyber Certification Level 1
        - ISO 27001:2022
            - As an ISO27001 certified organisation the Company has established, documented and maintains a Business Continuity and Disaster Recovery Policy and plans.
        - The policy documents and registers to support this contain sensitive information and are classified as RESTRICTED within the organisation's ISMS Policy framework.
        - Where it is necessary to disclose Business Continuity and Disaster Recovery with end user organisations the documents may be shared on a strictly confidential 1:1 basis.
        - The company reserves the right to redact areas of the documents shared that detail recovery processes or steps in order to protect critically sensitive areas of the business and to minimise risk of data compromise or further potential security breaches.
- Certification body:
    - CyberSmart is authorised as:
        - **Cyber Essentials** Certification Body
            - ID: 7bea3cc0-3801-418a-a3d5-62d41d6855f1
        - **Cyber Essentials Plus** Certification Body
            - ID: 0d4f2a37-d74a-4792-8a96-d880b4ba9c17

        - **IASME Cyber Assurance** Certification Body
            - ID: 9b9c1893-8f6c-4ef7-8494-c9bbf3dc23c0
        - **IASME Cyber Baseline Level 1** Certification Body
            - ID: 0a3e6170-3770-4681-ab86-79d6566c24b8
        - **Defence Cyber Certification** - Certification Body **Level 0**
            - ID: 62ed353c-bee1-4234-b533-152d2b2a64e8
        - **Defence Cyber Certification** - Certification Body **Level 1**
            - ID: f803ea02-5257-48f9-9ee2-577cb4224723
- Advisory:
    - CyberSmart is approved as:
        - Assured Service Provider - Cyber Advisor (Cyber Essentials)
            - ID: 72e45eef-dce8-4b42-b50b-92741ce78e84

Pricing Overview

- Pricing (all pricing excludes VAT on an annual subscription basis):
    - CyberSmart Core: CyberSmart Active Protect, Cyber Essentials certification, Patch and Learn Lite per organisation (based on organisation size):
        - 1-9 users: £1,025
        - 10-19 users: £1,340
        - 20-49 users: £2,285
        - 50-99 users: £3,205
        - 100-249 users: £4,750
        - 250-499 users: £8,280
        - 500-749 users: £12,375
        - 750-999 users: £15,445
        - 1,000+ users: £15.45/user
    - CyberSmart Complete: CyberSmart Active Protect, Cyber Essentials certification, Cyber Essentials Plus certification, Privacy Toolbox, Patch and Learn per organisation (based on organisation size):
        - 1-9 users: £2,716
        - 10-19 users: £3,255
        - 20-49 users: £4,205
        - 50-99 users: £5,520
        - 100-249 users: £8,190
        - 250-499 users: £11,880
        - 500-749 users: £17,305
        - 750-999 users: £20,375
        - 1,000+ users: £20.38/user
    - Cyber Essentials certification only per organisation:
        - Up to 10k employees: £675
        - Over 10k employees: £1,350

    - Cyber Essentials Plus certification only per organisation
        - 1-9 employees: £1,450
        - 10-49 employees: £1,650
        - 50-99 employees: £2,050
        - 100-499 employees: £3,095
        - 500-999 employees: £4,300
        - 1,000+ employees: £4,300 + day rate of £1,499 (may apply depending on scope and audit duration)
        - All prices +£350 where UK onsite audit required
        - NOTE: Cyber Essentials Plus requires Cyber Essentials to have been awarded within 3 calendar months of the date of submission for certification.
    - Defence Cyber Certification (DCC) only per organisation:
        - Level 0:
            - 1-9 employees: £876
            - 10-49 employees: £1,101
            - 50-249 employees: £1,548
            - 250-999 employees: £2,445
            - 1,000+ employees: £2,445 + day rate of £1,499 (may apply depending on scope and audit duration)
        - Level 1:
            - 1-9 employees: £4,176
            - 10-49 employees: £4,623
            - 50-249 employees: £5,070
            - 250-999 employees: £8,055
            - 1,000+ employees: £8,055 + day rate of £1,499 (may apply depending on scope and audit duration)
- Volume discounts:
    - Cyber Essentials: nil
    - Cyber Essentials Plus: nil
- Data extraction costs for all services - nil

Service Constraints

- Browser access
    - Chrome (recommended browser)
    - Firefox
    - Edge
    - Safari
- Operating systems supported:
    - Windows 11, 10, 8.1 (all editions)
    - MacOS (26 Tahoe - 10.12 Sierra)
    - Windows Server 2025, 2022, 2019, 2016, 2012, 2008 R2 (with Desktop Experience)
    - iOS 15.6+

    - Android 8.1+
- Operating systems not currently supported:
    - Linux
- Minimum Hardware Specification (Desktop)
    - 1GB RAM
    - 3.3+ GHz (Manufacturer example: Intel i3 3rd Generation, AMD Ryzen 3)
    - Ports:
        - If machines are able to access the internet, usually no additional configuration is required.
        - TCP 443 (All traffic is over secure web HTTPS)
        - UDP 53 (DNS lookups)
    - Restrictive firewalls whitelist:
        - Domains:
            - app.cybersmart.co.uk
            - cs-dapi.cybersmart.co.uk
- Check Boundaries:
    - The CyberSmart software predominantly checks native security configuration on devices and if any existing software installed on devices has any known vulnerabilities.
    - For the anti-malware and firewall checks, the software will also check for third party installs (e.g. Avira, Avast, Sophos, etc.) and include the name of the third-party user next to the check.
- By default, the software application operates in 'report-only' mode, meaning it cannot modify anything on the device, it simply reports information about security configuration settings and software vulnerabilities to your cloud-based dashboard.
- Maintenance windows:
    - The CyberSmart platform and cloud services are delivered on a 24/7/365 operating schedule.
- Customisation allowed:
    - Various features can be configured as required by the organisation administrator:
        - CyberSmart Learn Lite Email Reminders
        - Inactive devices cleaning
        - Feature switches:
            - CyberSmart Learn Lite
            - Smart Score
            - Active Protect Steps to Fix
            - Active Protect Vulnerable Software
            - Enforce Multi-Factor Authentication (MFA)

Data Access:

- The CyberSmart software application has been designed to collect minimal information in a privacy first manner, specifically relevant to meeting and maintaining security compliance requirements.
- The information CyberSmart will have access to:
    - Information related to the device:
        - Operating system

        - Device ID
        - Hostname
        - Serial number
        - Device configuration settings
        - Make and model of the device
    - Information related to the user:
        - Current username
        - Windows domain, if in use
        - If user is an admin or regular user
    - Information related to the network:
        - Network interfaces
    - Information related to installed software:
        - Software installed and version
    - Information relevant to diagnostics:
        - App version and install type
        - In the event of a crash, the error that occurred
- As CyberSmart expands app functionality we may look at additional data points to support our goal of making compliance more accessible and automated. We have no plans for this to include any personal, sensitive data or information being sent across the network.

Service Levels

- Performance
    - Availability: 99.9%
        - CyberSmart Service Commitment: 99.9% Uptime
            - CyberSmart will use commercially reasonable efforts to make your CyberSmart services available with a Monthly Uptime Percentage of at least 99.9% during any monthly billing cycle (the “Service Commitment”).
            - Subject to the SLA Exclusions, if we do not meet the Service Commitment, you will be eligible to receive a Service Credit. A Monthly Uptime Percentage of 99.9% means that we guarantee you will experience no more than 43.8 min/month of Unavailability.
        - Definitions
            - “Maintenance” means scheduled Unavailability of the Services, as announced by us prior to the Services becoming Unavailable.
            - “Monthly Uptime Percentage” is calculated by subtracting from 100% the percentage of minutes during the month in which the Services were Unavailable. Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any SLA Exclusion.
            - “Service Credit” means a credit denominated in GBP, calculated as set forth below, that we credit back to an eligible account.
            - “Unavailable” and “Unavailability” mean, for the CyberSmart web platform, when your dashboard is unreachable due to CyberSmart’s fault.
        - Service Commitments and Service Credits
            - Service Credits are calculated as a percentage of the total charges due on your CyberSmart invoice for the monthly billing cycle in which the

Unavailability occurred, applied proportionally to the Services that were Unavailable, in accordance with the schedule below:

- For Monthly Uptime Percentage less than 99.9% but equal to or greater than 99.0%:
    - you will be eligible for a Service Credit of 10% of the charges attributable to the affected resources.
- For Monthly Uptime Percentage less than 99.0%:
    - you will be eligible for a Service Credit of 30% of the charges attributable to the affected resources.
    - e.g. if you are unable to access the dashboard for 45 minutes, you would be eligible for a Service Credit for 10% of the usage for the month.
- We will apply any Service Credits only against future payments for the Services otherwise due from you.
- At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the Unavailability occurred.
- Service Credits will not entitle you to any refund or other payment from CyberSmart.

■ Sole Remedy

- Unless otherwise provided in the Terms, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide the Services is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

■ Credit Request and Payment Procedures

- To receive a Service Credit, you must submit a claim by emailing support@cybersmart.co.uk.
- To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include the words “SLA Credit” in the subject line as well as the dates and times of each Unavailability incident;
- If the Monthly Uptime Percentage of such a request is confirmed by us and is less than the Service Commitment, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us.

■ SLA Exclusions

- The Service Commitment does not apply to any Unavailability:
- That results from a suspension or Remedial Action, as described in the Terms;
- Caused by factors outside of our reasonable control, including any force majeure event, Internet access, or problems beyond the demarcation point of the CyberSmart network;
- That results from any actions or inactions of you or any third party;
- That results from the equipment, software or other technology of you or any third party (other than third party equipment within our direct control);
- That results from failures of Services not attributable to Unavailability; or
- That results from any planned Maintenance.

- If availability is impacted by factors other than those used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.

- P1 Incidents:
  - Issues involving errors resulting in 100% loss of functionality and no reasonable workaround is immediately available: OR
  - No organisation can perform one of the following:
    - Purchase product licences
    - Upgrade product licences
    - Provision or assign purchased licences
    - Raise billing via the platform
    - Submit for certification any product
  - P1 - Intervention time: 30 minutes (during business hours)
  - P1 - Workaround time: 8 hours
  - P1 – Final Fix time: 24 hours
- P2 Incidents:
  - Issues impacting critical features and functionality that restrict use and no immediate workaround is available: OR
  - Multiple (but not all organisations) cannot perform one of the following for at least one product:
    - Purchase product licences
    - Upgrade product licences
    - Provision or assign purchased licences
    - Raise billing via the platform
    - Submit for certification any product: OR
  - More than 10% of organisations, users or licences are affected and there is no published or available alternative workflow available.
  - P2 - Intervention time: 60 minutes (during business hours)
  - P2- Workaround time: 24 hours
  - P2 - Final Fix time: 10 business days
- P3 Incidents:
  - Issues where parts of the service or systems are not working properly for multiple users with low impact on users or organisations: OR
  - A single organisation has lost all functionality or access to the system
  - P3 - Intervention time: 48 hours
  - P3 - Workaround time: 5 business days
  - P3 - Final Fix time: 20 business days
- P4 - Incidents:
  - An issue has occurred that impacts a single user or impacts a rarely used device type with acceptable impact on the organisation or user.
  - P4 Intervention time: 72 hours
  - P4 - Workaround time: 10 business days

        - P4 - Final Fix time: 30 business days
- Availability
    - CyberSmart will use commercially reasonable efforts to make your CyberSmart services available with a Monthly Uptime Percentage of at least 99.9% during any monthly billing cycle (the "Service Commitment").
    - Subject to the SLA Exclusions, if we do not meet the Service Commitment, of 90% available within any monthly billing cycle you will be eligible to receive a Service Credit.
- Support Hours
    - Email support:
        - Monday to Friday 09:00 - 18:00 excluding UK (England) Bank Holidays.
    - Webchat support:
        - Monday to Friday 09:00 - 18:00 excluding UK (England) Bank Holidays.
    - Online knowledge portal: 24/7/365
- Compensation for substandard service levels
    - Repay or compensate buyers

Ordering and Invoicing Processes

- Ordering:
    - Orders can be placed via the CyberSmart website at https://app.cybersmart.co.uk/signup ;
    - All major credit / debit cards accepted - direct debit mandate accepted;
    - If you require a PO before purchase, please email finance@cybersmart.co.uk.
- Invoicing:
    - A digital invoice in pdf format will be emailed to the email address provided on registration and held on file by CyberSmart;
    - Historic invoices are available through the CyberSmart platform;
    - Invoicing queries to be addressed to finance@cybersmart.co.uk or support@cybersmart.co.uk .
- Termination of a contract
    - Buyers of the products and services can terminate their contract by:
        - The contract for Cyber Essentials is deemed complete on the date of achieving certification. Any outstanding fees fall due on this date.
        - The contract for Cyber Essentials Plus is deemed complete on the date of achieving certification. Any outstanding fees fall due on this date.
        - The contract for IASME Governance is deemed complete on the date of achieving certification. Any outstanding fees fall due on this date.
        - Access to the certification platform for the retrieval of any issued electronic certificate (Cyber Essentials, Cyber Essentials Plus, IASME Governance), entitled certification logos, badges or other artefacts and the technical auditor's report is available post termination, for a period up to and including the final date of certification.
    - Notifying CyberSmart Ltd:
        - All termination of services must be submitted to CyberSmart Ltd:
            - In writing to the registered address: 68-80 Hanbury Street, London E1 5JL, giving no less than 1 calendar months notice of termination;

                OR

        - By email to support@cybersmart.co.uk giving no less than 1 calendar months notice of termination.
    - All termination notices to be clearly titled: Notice to Request Termination of G-Cloud service.
    - Notices to terminate by phone or webchat contact cannot be accepted and callers will be advised by CyberSmart Ltd that they are to submit their formal notification in writing or by email using the details above.
    - In all termination events, CyberSmart Ltd reserves the right to contact the organisation directly for clarification and authority to proceed with termination of any or all services, where the person or agent requesting termination is not the account administrator as registered against any service.
    - Where termination is executed prior to the award of any certificate service, CyberSmart Ltd reserves the right as a Certification Body to withhold submission of the application for certificate award.

After Sales Support

- CyberSmart delivers live customer support and after sales support as follows:
    - CyberSmart run live customer support and after sales support as follows:
        - Email support:
            - Monday to Friday 09:00 - 18:30 less UK (England) Bank Holidays.
        - Webchat support:
            - Monday to Friday 09:00 - 18:30 less UK (England) Bank Holidays.
        - Online knowledge portal: 24/7/365
    - Reporting product or service issues:
        - Email support:
            - Monday to Friday 09:00 - 18:30 less UK (England) Bank Holidays.
        - Web Ticket system:
            - 24/7/365

Technical requirements

- To access the service or product the customer or end user will require:
    - For Cyber Essentials
        - Access to the internet via any of the following browsers:
            - Chrome
            - Edge
            - Safari
            - Firefox
        - An issued username and password
        - The service can be accessed via mobile phone or tablet devices, but it is recommended that users access via a laptop or desktop device.
        - The platform is WCAG 2.0 compliant for visually impaired access.
    - For Cyber Essentials Plus
        - Access to the internet via any of the following browsers:
            - Chrome

- Edge
- Safari
- Firefox

- An issued username and password
- The service can be accessed via mobile phone or tablet devices, but it is recommended that users access via a laptop or desktop device.
- The platform is WCAG 2.0 compliant for visually impaired access.
- For onsite auditing, the organisation will be required to provide site access, as identified by the Auditor, and access to a systems administrator with permission to configure identified devices or systems for access to the CyberSmart auditor for a period limited to the performance of the audit.
- For remote auditing, the organisation will be required to provide access to a systems administrator with permissions necessary to deploy approved auditing software for the limited purpose and period of the audit.
- For on-site and remote auditing purposes the CyberSmart Auditor will during the discovery phase of achieving certification notify the organisation of all the identified audit requirements a minimum of 72 hours in advance.
- In the event of any re-auditing necessary to demonstrate corrective actions have been taken to achieve the necessary certification standard, the organisation may be required to extend the auditing on-site or remote auditing access privileges.

- For CyberSmart Active Protect
  - An account with CyberSmart to enable provisioning of apps to devices
  - An organisation administrator to authorise and trigger application deployment to user devices in any of the two authorised deployment methods as chosen by the organisation:
    - Individual deployment: or
    - Bulk organisation deployment
  - Desktop devices with the following operating systems:
    - Windows 11, 10, 8.1 (all editions)
    - MacOS (26 Tahoe - 10.12 Sierra)
    - Windows Server 2025, 2022, 2019, 2016, 2012, 2008 R2 (with Desktop Experience)
  - Mobile devices with the following operating systems:
    - iOS 15.6+
    - Android 8.1+
  - When deployed to a desktop or mobile device the application is available 24/7 to the device user.
  - Where devices have password protection systems in place the application will only be available to the device user, when the device user has entered their unique password and gained access to the device.
- For the CyberSmart Cloud Based Administrative Dashboard
  - An account with CyberSmart that permits access to the Cloud Based Administrative Dashboard
  - Access to Dashboard via the internet using any of the following browsers:
    - Chrome

- Edge
- Safari
- Firefox

- An issued username and password
- The service can be accessed via mobile phone or tablet devices, but it is recommended that users access via a laptop or desktop device.
- The platform is WCAG 2.0 compliant for visually impaired access.