CfA Centre for Assessment	Terms and Conditions	Date: 12/11/2026
		Revision: 6

This document applies to clients involved in the following standards: Cyber Essentials, Cyber Essentials Plus & Cyber Esentials Plus Extra. These terms & conditions form an agreement between CfA and its client organisations.

1. The Scope of these Terms and Conditions

a) Centre for Assessment Limited (**CfA**) conducts assessments and certification of documented management systems against Internationally Recognised Standards. **Customers** certified by CfA are required to comply with the specifications of these terms and conditions for the duration of their certification.

b) The certification service is available to all applicants regardless of the size, location and membership of their group or association.

2. Background

a) The Scope of assessment issued by IASME, acknowledges that CfA has the knowledge and skills to manage assessments for Cyber Essentials.

b) The Cyber Essentials scheme is owned by HM Government (the authority), IASME is the accreditation body and CfA are the certification body.

3. Personnel / Confidentiality

a) CfA will treat all aspects of the Assessment as 'commercial in confidence' and any information/evidence outside of the public domain that is gained during the assessment will be used for the purpose of the assessment only.

b) CfA will provide suitably qualified personnel for all assessment types. CfA reserve the right to use partner organisations who are registered with IASME to conduct parts of the assessment on a subcontracted basis. CfA employees, their Partners and sub-contractors are required to sign contracts, which contain confidentiality agreements, requiring them to treat all information outside the public domain as 'commercial in confidence.'

c) The organisation will be responsible for the assessors and any observers appointed by CfA, health and wellbeing whilst on their premises and must provide a safe environment for them to conduct the assessment in.

d) CfA or its Accreditation Body may be required to accompany assessors on assessments to evaluate consistency and quality of practice within the assessment team. The organisation will be informed in writing that the Assessor will be accompanied. Any personnel in attendance will be subject to confidentiality agreements.

e) Details on how the Customer's data is used is available in CfA privacy policy which can be viewed on our website https://www.centreforassessment.co.uk/privacy-policy/ or requested in writing to enquiries@centreforassessment.co.uk.

f) If CfA employees and/or their subcontracted assessors/technical experts are made aware of any form of breaking the law during the assessment they are obliged to inform the regulatory bodies or relevant law enforcement agency.

4. Conflict of Interest

a) Organisation are required to inform CfA of any conflict of interest or potential conflict of interest relating to the assessment before the assessment takes place in writing to enquiries@centreforassessment.co.uk.

5. Application for Assessment

a) The assessment for certification will be conducted only on the basis that the Customer have paid the fees in full and that the Customer accept the terms and conditions of this agreement in full. If the Customer have not submitted the Customer's assessment application within 6 months, CfA are under no obligation to conduct an assessment and no refund will be issued. After this time, the Customer will need to start the process again and another fee will be applicable.

6. Applications Forms/Accurate Information/Additional Fees

a) Information provided to CfA and/or the assessor must be correct and accurate. If the assessor finds that the information is not correct during the assessment additional fees will be applicable

b) Any additional fees will be discussed with the client organisation, and should they choose to terminate the assessment at this stage then the original quote will be chargeable, but the organisation will not be accredited to Cyber Essentials /Plus.

c) If the Customer's devices are not networked and the assessor must conduct multiple scans this will incur additional fees

7. Cyber Essentials Plus/Extra

a) On receiving an initial enquiry, CfA will issue a quotation confirming the assessment costs. This will be followed by a telephone call to answer any questions and confirm the organisation intention to proceed.

b) CfA will assign an Assessor(s) who will act on behalf of CfA

i) An email will be sent to the organisation containing relevant forms that must be read and signed by a person within the organisation who has authorisation to sign such forms. CfA do not take responsibility for forms that have been signed by unauthorised personnel.

ii) The organisation is required to provide accurate information in these forms to allow the assessment to take place. Should in accurate information be provided the assessment may be deemed void and the organisation will need to re-apply incurring further assessment costs.

iii) Testing of the organisations systems will mainly be done remotely but an onsite visit at the client's premises may be required to do this. The organisation will be advised in advance if this is the case and suitable dates will be arranged. These are required to be within 6 months of the original application form being submitted.

iv) If the Customer's Assessment meets the Scheme criteria (which CfA shall assess at our sole and absolute discretion) CfA will notify the Customer by phone or by email and, subject to the Customer meeting the Customer's obligations under clause 2, will arrange for the issue of a Scheme Certificate to the Customer.

v) If the Customer do not meet the requirements of the standard, the Customer will be given feedback on the areas that the Customer did not meet the standard

8. Certification (All assessment Types)

a) On completion of the assessment, the organisation will receive their certificate from our accreditation body IASME. This will be sent electronically to the **email address supplied in the application form.**

9. Cyber Essentials Registers

a) The Customer will be entered on the National Register of Cyber Essentials Certified Companies, the National Register may take up to 6 weeks to populate.

10. Renewal of Cyber Essentials Basic/Plus

a) The Customer's certificate is valid for 12 months and will need to be renewal assessment prior to the expiry date on the Customer's certificate or the Customer's certification will lapse. Please note it is the organisation responsibility to ensure that they submit an application form at least 4 weeks prior to their certificate expiry.

b) CfA do not take any responsibility for expiring certificates or and do not accept liability for any costs associated to this.

11. Changes to the Customer's system

a) If the Customer's systems configuration changes in a way that the answers in the Customer's questionnaire would have been answered differently, then the Customer may need to re-apply for recertification early.

12. Changes in Organisation/Firm

a) CfA should be informed in writing of any relevant changes to the organisation (including merger, change in ownership or structure) which may affect future their certificate assessments. In such an event, CfA reserves the right to request that the organisation for re-Assessment. Organisations are required to ensure that they notify us of any contact details changing in personal, email addresses and telephone numbers.

13. Certificates and Trademarks

a) Certificates and Trademarks will be issued by the accreditation body and are subject to the Terms and Conditions of use and brand guidance which must be followed when displaying certificates or using trademarks/Logos on literature/website or any other form of advertising.

14. Suspension or Withdrawal

a) The organisations Cyber Essentials Certificate may be deferred, withdrawn, withheld or suspended for but not limited to the following reasons:

   i) Breach of any of these Terms & Conditions of Registration.

   ii) Failure to have annual visits or meet the requirements of the Cyber Essentials standard

   iii) Failure to apply corrective action as a result of non-conformities found at Assessment

   iv) Continued Trademark Misuse.

   v) Suspected or found to be in flagrant breach of Cyber Essentials

   vi) Committed fraud or serious professional misconduct

   vii) Bringing the standard into disrepute in any way.

   viii) Failure of the organisation/firm to settle any outstanding CfA Invoices

   ix) Failure to provide copies of documentation required by the assessor(s) to undertake re-assessment

b) In the event of withdrawal or suspension of certification the organisation shall discontinue the use of all advertising, internet and brochures that contain reference to the Cyber Essentials Standard. The organisation shall return their certificate to the Cyber Essentials Office; and the Cyber Essentials Mark must no longer be used in the public domain or internally.

15. Certificate Misuse

a) The organisation must not misuse the certificate in any way or attempt to change the dates or deface the certificate in organisations advertising. Any findings of certificate misuse will be reported to the accreditation body

16. Publicity

a) Once a certificate has been awarded, organisation have the right to publicise their award. Appropriate logos may be used on stationery and in marketing or promotional material. Any reference to CfA must not contain any claims that are misleading or bring CfA or the Cyber Essentials standard into disrepute.

17. Scheme Reputation

a) Organisations must agree that they will not make any derogatory statements about the standard or behave in any manner that would damage the reputation of the Scheme.

b) CfA reserve the right to publish an organisation award on their website/ and or social media unless the firms advises in writing within 3 days of notification of their award.

18. Appeals Procedure

a) If for any reason the organisation does not agree with the outcome of the assessment, they may appeal in the first instance by contacting the Operations Manager of CfA.

19. Complaints against CfA, Employees or Sub-contractors

a) If an organisation has a complaint, it should be addressed in writing to the Operations Manager of CfA. Where the complaint involves the Operations Manager, it should be addressed in writing to the Managing Director of CfA.

b) An initial response to the complaint will be received within 10 working days of the complaint being received and a resolution will be sought to be met within 60 days unless otherwise informed.

20. Costs

a) Costs for assessment should be agreed in advance between CfA and the organisation. **Invoices will be sent via email from our finance department** finance@growthco.uk

b) Once the assessment has started the costs quotes are required in full

c) **VAT**: All quotes and estimated costs for all services will be plus VAT. Customers who are VAT registered outside of the UK but within the EU must provide their VAT registration number to CfA before any work takes place. If this is not received then VAT will be added to their invoice.

21. Travel Expenses

a) Travel expenses may be applicable dependant on organisation location, number of sites and Local Assessor availability. Any expenses to be incurred will be agreed between the Assessor and the organisation before the assessment takes place. Mileage will be calculated at £0.55 per mile; and any overnight expenses will be charged at cost. These costs will be included in the final invoice**.**

22. Payment of Invoices

a) Payments for Cyber Essentials Basic are required prior to the assessment taking place. Payment for Cyber Essentials Plus /Plus Extra will be required with 30 days of the invoice being issued. Certificates will not be issued until payment has been received.

b) Late payment of invoices will automatically be referred to our legal department for perusal and may result in accreditations being removed.

23. Additional Visit

a) A fee which is proportionate to the additional work required should be agreed by both parties in advance. (An additional visit may be required when a site visit identifies either a major issue to be addressed, or information, which differs from that contained in the initial application, such as the number of sites or number of employees).

24. Cancellation policy

a) CfA operates a strict cancellation policy. If an assessment or annual maintenance visit is cancelled by the organisation within 30 days of the agreed visit date(s), CfA reserves the right to claim the appertaining daily assessment charge for each scheduled day on-site.

25. Warranty

a) The Client Organisation warrants that

i) the Scheme Questionnaire has been completed by an authorised and suitably competent person.

ii) it will maintain the Security Profile indicated in the Customer's completed Questionnaire.

iii) the Scheme Questionnaire submitted is complete and accurate in all material respects.

iv) it acknowledges the Scheme is intended to reflect that certificated organisation have themselves established the cyber security profile set out in the Scheme documents only and that receipt of a Scheme Certificate does not indicate or certify that the certificate holder is free from cyber security vulnerabilities.

v) It acknowledges that CfA has not warranted or represented the scheme or certification under the scheme as conferring any additional benefit to the Client Organisation.

26. Limitation of Liability

a) CfA does not accept any liability to the Customer resulting from any security breach or vulnerability in the Customer's systems or processes.

b) Without prejudice to the generality of clause above, CfA shall not be liable to the Customer whether in contract, tort (including negligence) for breach of statutory duty or otherwise arising under or in connection with this agreement for:

i) loss of profits;

ii) loss of sales or business;

iii) loss of agreements or contracts;

iv) loss of anticipated savings;

v) loss of or damage to goodwill;

vi) loss of use or corruption of software, data or information;

vii) any indirect or consequential loss.

c) Assessments undertaken by CfA address only a sample of the organisation System. Findings reported do not imply that the issues raised are the only ones which exist. Any action taken by the organisation as a result of assessment work undertaken on behalf of CfA remains the responsibility of the organisation.

27. IT Systems

a) The Assessor(s) may complete electronic reports on site and may need the use of aa secure WIFI network. All assessment personnel are required to keep their personal IT system virus free with up-to-date viral protection, but should a problem arise, CfA cannot accept responsibility for any corruption of the organisation IT systems. The organisation has the right to refuse access to their IT Systems.

28. Indemnity

a) The Organisation will indemnify CfA against any claims or losses suffered by CfA as a result of misuse by the Organisation of Certification given by CfA.

29. Termination

a) CfA may terminate the certification process at any stage without notice to the Customer in the event that the Customer are in breach of any of the Customer's obligations under this agreement.

30. Prevention of harassment of CfA Personnel

a) The Client Organisation acknowledges that CfA has obligations under the Employment Rights Act 2025, including section 21, and the Equality Act 2010 to take all reasonable steps to prevent the harassment of its employees by third parties.

b) For the purposes of this clause, CfA Personnel means CfA's employees, auditors, assessors, contractors and associates involved in the delivery or administration of the Services.

c) The Customer shall ensure that its employees, officers, workers, agents and contractors, and any other persons under its control who may interact with CfA Personnel in connection with the Services (Customer Personnel), treat CfA Personnel with dignity and respect and do not engage in harassment, sexual harassment, bullying, discrimination, threatening or abusive behaviour, or other inappropriate conduct towards CfA Personnel.

d) The obligations in this clause apply to all communications and interactions between CfA Personnel and Customer Personnel, regardless of location and whether in person, by telephone, email, video conference, messaging service or through any other communication channel.

a) The Customer shall promptly notify CfA if it becomes aware of any allegation or incident of conduct falling within clause 30 c) involving Customer Personnel and CfA Personnel. The Customer shall co-operate reasonably with CfA in investigating any such allegation or incident and shall implement appropriate measures to address the matter and prevent recurrence.

b) Where CfA reasonably considers that conduct towards CfA Personnel is unacceptable, or that there is a risk to their safety or wellbeing, CfA may take such reasonable action as it considers necessary to protect CfA Personnel.

c) Where the provision of the Services is suspended, terminated, rearranged or rescheduled as a result of conduct falling within clause 30 c), the Customer shall be responsible for any reasonable additional costs incurred by CfA as a result, subject to any other applicable provisions of these Terms and Conditions.

d) The Customer shall indemnify and hold harmless CfA against all costs, claims, damages, or expenses incurred by CfA arising from any act of harassment or other such conduct of a similar nature committed by the Customer's Personnel against CfA's Personnel.

e) Serious or repeated failure by the Customer to comply with this clause may constitute a material breach of these Terms and Conditions and may result in CfA suspending the provision of the Services or exercising any other rights or remedies available to it under these Terms and Conditions.

31. Other Services

a) CfA reserve the right to approach Organisation about other services that they provide that they deem of interest to the organisation.

32. Data Protection Statement

a) The information the Customer provide to us, or our sub-contractors, will be used in the delivery of services to the Customer's business.

33. <u>Data protection Statement</u>

a) All information gathered by CfA in the delivery of its services is processed in accordance with the Data Protection Act 2018. For further information on how CfA processes the Customer's personal data please see our privacy policy which is located on our website **CfA Privacy Notice**

b) For the purpose of these terms and conditions CfA will act as the processor and the client organisation will be the controller

c) The Customer's data will only be passed to a 3rd party when it is needed to preform and complete the contract that has been entered into. e.g., Cyber Essentials Assessment and Certification. 3rd parties include but are not limited to: IASME, The National Cyber Security Centre, CfA subcontracted assessors, our Cyber Essentials Assessors, our Service Partners and subcontracted assessors, and the Customer's IT Support Company.

34. Terms and Conditions

a) These terms and condition's form a legally binding contract. Any validity and performance of the contract shall be governed in all respects by English Law; in connection with any disputes between the parties relating to or connected with the assessment contract; both parties shall agree irrevocably to submit to the non-exclusive jurisdiction of the Supreme Court of Judicature in England.

35. Terms & Conditions Variation

a) CfA reserves the right to change these Terms and Conditions. Due notice will be given for any changes to these requirements.