



Supplementary Terms for the supply of Cyber Essentials Assessment Services

The Services set out in these Supplementary Terms shall be supplied by Holistic IT to the Client on the terms and conditions set out in Holistic IT's General Terms and Conditions and those of these Supplementary Terms.

1. SUPPLEMENTARY DEFINITIONS

- 1.1 'Accreditation Period' means the period of validity of the accreditation following Cyber Essentials or IASME Governance and GDPR Assessment.
- 1.2 'Assess', 'Assessment' means the assessment, by Holistic IT, of the Client's Security Profile against the Scheme.
- 1.3 'Audit' means Holistic IT's checking of a sample of the Client's IT systems, devices or processes or policies to verify the Client's responses to the Questionnaire.
- 1.4 'Security Profile' means the Client's cyber security posture / stance at the time of Holistic IT's Assessment.
- 1.5 'Certification Body' means an organisation which has been appointed by the Accreditation Body to deliver the Scheme.
- 1.6 'Self Assessment Questionnaire' or 'Questionnaire' means the questionnaire used for the assessment of the Client's compliance with the Scheme.
- 1.7 'Site' means the Client- owned or occupied location(s) as set out in the Order, at or to which Holistic IT shall carry out or otherwise supply the Assessment Services.
- 1.8 'Vulnerability Test' or 'Vulnerability Testing' means an automatic or manual check of the Client's systems configuration pertaining to cyber security which is performed by Holistic IT.

2. TERM

- 2.1 This Agreement will be effective from the Commencement Date set out on the Order and shall run until terminated in accordance with the provisions of clause 9 hereof.

3. BACKGROUND

- 3.1 The Cyber Essentials Scheme and the IASME Governance Scheme (collectively, the 'Scheme') are owned by HM Government (the 'Authority') and the IASME Consortium Ltd respectively. The Scheme's delivery is overseen by the IASME Consortium Ltd (the 'Accreditation Body'). Holistic IT's supplier has been approved by the Accreditation Body for delivery of the Scheme.
- 3.2 Holistic IT's assessment services (the 'Assessment Services') comprise delivery a number of certification levels (the 'Certification Level') of the Scheme and a number of value-added services (the 'Assistance Level'), which are described in the Service Schedule.
- 3.3 On successful completion of the Assessment, Holistic IT shall issue to the Client a certificate (the 'Scheme Certificate') and the Client, subject to agreeing to the Accreditation Body's terms and conditions for the use of the appropriate logo, (the 'Accreditation Mark'), shall be entitled to display the Accreditation Mark on its literature, website, etc.
- 3.4 The Scheme Certificate shall be valid for a period of twelve months from the date of issue by Holistic IT and the Client shall be entitled to use the Accreditation Mark during the period of validity of the Scheme Certificate.

- 3.5 In order to maintain continuity of certification, the Client must apply for and complete further Assessments of the Security Profile, the requirements for which are specific to each Certification Level and are outlined in the Service Schedule and fully documented in the Scheme documentation.

4. PROVISION OF SERVICES

The Assessment Services to be supplied under the terms of this Agreement comprise a Certification Level and an Assistance Level, as set out in the Order and described in the Service Schedule:

- 4.1 The Certification Levels are:
- 4.1.1 Cyber Essentials;
 - 4.1.2 Cyber Essentials Plus;
 - 4.1.3 IASME Governance and GDPR.
- 4.2 Holistic IT's Assistance Levels are:
- 4.2.1 Independent Certification;
 - 4.2.2 Independent and Checked Certification;
 - 4.2.3 Pre-assessed and (Holistic) Engineer Completed Certification.
- 4.3 Some Certification Level / Assistance Level combinations are mutually exclusive.

5. CLIENT'S OBLIGATIONS

During the term of this Agreement, the Client shall:

- 5.1 Warrant that the Self Assessment Questionnaire shall be completed honestly and accurately by person(s) who are authorised and qualified to provide the requested information.
- 5.2 Warrant that information provided to Holistic IT during any Audits shall be provided honestly and accurately by person(s) who are authorised and qualified to provide the requested information.
- 5.3 Comply with the requirements of the Scheme documentation and all reasonable directions made by the Authority, the Accreditation Body and Holistic IT.
- 5.4 Acknowledge and agree that any Scheme Certificate shall only be issued by Holistic IT when Holistic IT, at its sole discretion is satisfied that the Client meets the criteria set out by the Authority.
- 5.5 Not use the Accreditation Mark unless in receipt of a valid, current Scheme Certificate as issued by Holistic IT.
- 5.6 Enter into an agreement with the Accreditation Body prior to the use of the Accreditation Mark and comply with all terms and conditions of such agreement.
- 5.7 Warrant that Security Profile indicated in the completed Self Assessment Questionnaire shall be maintained for the duration of the Accreditation Period.
- 5.8 Complete the Assessment, including any re-Assessments following failed Assessments, within six months of the Commencement Date.
- 5.9 Within ten Working Days of any request for an appointment made by Holistic IT for the purpose carrying out the Assessment, including Audits or Vulnerability Tests, agree an appointment date.
- 5.10 Prior to the agreed date for any Vulnerability Test, provide to Holistic IT the necessary administration credentials to allow it to carry out the test.
- 5.11 Notify Holistic IT immediately and in any event with not less than one Working Day beforehand if the Client wishes to cancel a previously made appointment.
- 5.12 Prior to the agreed date for any Vulnerability Test, provide to Holistic IT the necessary administration credentials to allow it to carry out the test.
- 5.13 Pay any additional Charges reasonably levied by Holistic IT.

- 5.14 Not copy, reverse engineer or modify any software or copy any manuals or documentation, (save updating templates as required as part of the Assessment process) provided by Holistic IT under the terms of this Agreement.
- 5.15 Not make any derogatory statements about the Scheme or behave in any manner that could damage the reputation of the Scheme.

6. HOLISTIC IT'S OBLIGATIONS

During the term of this Agreement, and subject to the performance by the Client of its obligations hereunder, Holistic IT shall:

- 6.1 On commencement of this Agreement, make available to the Client the Self Assessment Questionnaire.
- 6.2 Provide the Client copies of all documentation required to assist its completion of the Assessment and where such documentation exists only on a web interface, access to such.
- 6.3 Provide to the Client assistance with the Assessment according to the Assistance Level set out on the Order and described in the Service Schedule.
- 6.4 Assess, at Holistic IT's sole discretion, the completed Self Assessment Questionnaire against the Scheme's criteria.
- 6.5 Agree dates and times for carrying out on-site Audits and Vulnerability Testing.
- 6.6 Carry out on-site Audits which shall be conducted and assessed at Holistic IT's sole discretion.
- 6.7 Carry out Vulnerability Tests at the agreed date and time, which shall be conducted and assessed at Holistic IT's sole discretion and notify the Client when such are complete.
- 6.8 Notify the Client in writing of the results of the Assessment; and
 - 6.8.1 If the Assessment meets the Scheme's criteria and subject to full payment of Holistic IT's Charges, issue a Scheme Certificate, which shall be valid for a period of twelve months from the date of issue;
 - 6.8.2 If the Assessment fails to meet the Scheme's criteria, Holistic IT shall not issue a Scheme Certificate. The Client shall be entitled re-apply for one additional Assessment at no further charge, PROVIDED THAT any and all Assessments are completed (including re-assessment by Holistic IT) within six months of the Commencement Date; and
 - 6.8.3 Whilst Holistic IT shall not charge the Client for carrying out parts of the additional Assessment that it can execute remotely, Holistic IT shall be entitled to charge the Client at its prevailing rates for any visits to the Client's Site that it reasonably deems necessary to make the additional Assessment;
 - 6.8.4 Holistic IT shall be entitled to charge the Client at its prevailing rates for carrying out any Assessments in excess of those identified in sub-clause 6.8.2.
- 6.9 Make available an account or project manager as appropriate to act as a single point of contact for the Client for the duration of this Agreement.
- 6.10 Perform the assessment of the Self Assessment Questionnaire, any on-site Audits and Vulnerability Testing using Good Industry Practice.
- 6.11 Facilitate the moderation of Assessments by the Accreditation Body where appropriate to the Assistance Level.

7. Clause Intentionally Unused

8. GENERAL

- 8.1 The Client acknowledges that the Scheme is intended to reflect that certificated organisations have themselves established the Security Profile set out in the Scheme documents and that receipt of a

Scheme Certificate does not indicate or certify that the certificate holder is free from cyber security vulnerabilities or their attendant risks; and

- 8.1.1 The Client also acknowledges that Holistic IT has not warranted or represented the Scheme or certification there under as conferring any additional benefit to the Client.
- 8.2 If, following submission of a Questionnaire for Assessment, Holistic IT requests further information, the Client should read the request for further information carefully and provide the detailed information requested; and
 - 8.2.1 The Client must provide the further information within two Working Days of the request being made; and
 - 8.2.2 Failure to comply with the provisions of sub-clause 8.2.1 shall result in the Assessment being deemed to have failed.
- 8.3 If the Client's first Assessment fails, exclusive of any Charges that may be levied by Holistic IT for additional assistance or consultancy that may be requested by the Client, the Client may re-submit a revised Questionnaire for re-Assessment within two Working Days of notice of the failure, at no extra Charge; however:
 - 8.3.1 The Client acknowledges that the free of charge re-Assessment offer is extended to the Client by the Accreditation Body on a "once only per company" basis and therefore its benefit cannot be realised if:
 - a) Following a failed Assessment a new Order is placed by the Client for further Assessment Services;
 - b) Following a failed Assessment the Client places an order for assessment services with an alternative Certification Body;
 - c) The Client has previously failed an Assessment which was carried out by another Certification Body.
- 8.4 Holistic IT will make an additional Charge for re-Assessment if the Questionnaire is re-submitted later than two Working Days after notification of the first failure of the first Assessment.
- 8.5 If during the completion of a Questionnaire or following a failed Assessment, the Client requests assistance or other consultancy, Holistic IT shall at its discretion provide such, which will be chargeable at its prevailing rate.
- 8.6 Notwithstanding that Holistic IT shall carry out applicable pre-Assessment of the Questionnaire with the appropriate skill and care, Holistic IT cannot guarantee that the formal Assessment will be successful and Holistic IT shall accept no liability should such situation arise.
- 8.7 If an appointment is made with the Client for a visit to Site and that at the appointed time Holistic IT is unable to access the Client's Site, or the appointment is otherwise broken by the Client within twenty four hours of the appointment time, Holistic IT shall be entitled to charge the Client at its prevailing rate.
- 8.8 Notwithstanding the provisions of clause 20 of the General Terms and Conditions, the Client agrees that the IASME Consortium Ltd and / or the Authority may at their discretion and without further authorisation publish the Client's company name and Certification Level on their respective websites.

9. TERMINATION

- 9.1 This Agreement shall terminate twelve months after the Commencement Date or at the end of the Accreditation Period, whichever is later, unless otherwise agreed in writing.
- 9.2 Unless otherwise agreed in writing, this Agreement shall terminate following an Assessment failure where there the Client has no remaining entitlement to re-Assessment (as contemplated in sub-clause 8.3) or third pre-Assessment failure; whereupon the Client may place a new Order for Assessment Services and commence a new agreement.

- 9.3 This Agreement may be terminated forthwith by Holistic IT if, in Holistic IT's reasonable opinion, the Client is in breach of sub-clauses 5.1 to 5.3 hereof.
- 9.4 The Scheme Certificate may be cancelled forthwith if in the Accreditation Body's reasonable opinion, the Client is in material breach of either this Agreement or any agreement with the Accreditation Body.

10. CHARGES AND PAYMENT

- 10.1 The Charges for the Assessment Services shall be paid in advance of the supply of the initial Assessment.
- 10.2 Charges for re-Assessment and subsequent renewal of the Scheme Certificate may be paid after the subsequent Assessment.
- 10.3 The Charges for the Assessment Services include the issue of one Scheme Certificate. If either additional copies of the Scheme Certificate or changes to the Scheme Certificate (for example, to the Client's address) are required, such will be charged at Holistic IT's prevailing rate.
- 10.4 The Charges are not refundable for any reason, save termination under the applicable terms of sub-clause 11.1 of the General Terms and Conditions arising from breach, action or inaction by Holistic IT.

11. EXCLUSION OF LIABILITY

- 11.1 The Client agrees that Holistic IT shall not be liable for any actions, losses damages, judgements, legal fees, costs, fines, claims or expenses incurred by the Client or legal proceedings which are brought or threatened against the Client by a third party in the event of:
 - 11.1.1 Any breaches by the Client of any Data Protection Regulations that is in force;
 - 11.1.2 Any security breach of or vulnerability in the Client's systems and processes.
- 11.2 The Client acknowledges and agrees that:
 - 11.2.1 There is a small risk that Vulnerability Testing carried out by Holistic IT may cause problems in the Client's IT systems, including routers and / or firewalls ceasing to function correctly and database and storage access issues;
 - 11.2.2 The testing of the Client's IT systems for correct functioning after Holistic IT's Vulnerability Testing and any necessary reconfiguration and any associated costs shall be the Client's sole responsibility;
 - 11.2.3 Whilst Holistic IT warrants that it shall use reasonable care during the execution of Vulnerability Tests, Holistic IT shall not be liable for any losses or damage which arise either directly or indirectly from its access to the Client's IT infrastructure.
- 11.3 The provisions of this clause 11 shall survive the termination of this Agreement in perpetuity.

Service Schedule

The following Service Schedule sets out all of the Assessment Services that may be provided by Holistic IT. The actual Assessment Services to be provided under the terms of this Agreement are listed on the Order.

1. Assistance Levels

1.1 Independent Certification

Under its Independent Certification Assistance Level, Holistic IT will provide the Client with access to the Self Assessment Questionnaire, which the Client will complete without any further assistance from Holistic IT. On completion of the Self Assessment Questionnaire by the Client, Holistic IT will Assess the completed Self Assessment Questionnaire and report the result of the Assessment to the Client. If the Assessment result meets the criteria of the Scheme, Holistic IT will issue a Scheme Certificate.

If the Assessment fails to meet the Scheme's criteria, the Client may submit one further Self Assessment Questionnaire for Assessment subject to the provisions of sub-clauses 8.3 and 9.2.

If technical assistance is required by the Client (that is, regarding making changes to the Client's systems or processes), such is not covered under the terms of this Agreement; however Holistic IT will in response to specific requests by the Client provide technical assistance and such will be chargeable at Holistic IT's prevailing rate.

1.2 Independent / Checked Certification

Under its Independent / Checked Certification Assistance Level, Holistic IT will provide the Client with access to the Self Assessment Questionnaire, which the Client will complete without any further assistance from Holistic IT. On completion of the Questionnaire by the Client, Holistic IT will pre-Assess the completed Questionnaire. If the pre-Assessment result meets the criteria of the Scheme, Holistic IT will formally Assess the Questionnaire and report the result of the Assessment to the Client. Provided that the Assessment result meets the criteria of the Scheme, Holistic IT will issue a Scheme Certificate.

If the pre-Assessment fails to meet the Scheme criteria, the Client may submit up to two further Self Assessment Questionnaires for pre-Assessment within six months of the Commencement Date; if after the third pre-Assessment the responses to the Questionnaire do not meet the Scheme criteria, this Agreement will terminate.

If the formal Assessment fails to meet the Scheme's criteria, one further Self Assessment Questionnaire may be submitted for Assessment subject to the provisions of sub-clauses 8.3 and 9.2.

If as a result of any pre-Assessment or Assessment, technical assistance is required by the Client (that is, regarding making changes to the Client's systems or processes), such is not covered under the terms of this Agreement; however Holistic IT will in response to specific requests by the Client provide such technical assistance and such will be chargeable at Holistic IT's prevailing rate.

1.3 Pre-assessed and (Holistic) Engineer Completed Certification

Under its Pre-assessed and (Holistic) Engineer Completed Certification Assistance Level, Holistic IT will complete the Self Assessment Questionnaire on behalf of the Client, based on its knowledge of the Client's IT infrastructure and security posture. Any questions that Holistic IT is unable to answer will be referred to the Client for clarification. On completion of the Questionnaire, Holistic IT will pre-Assess the completed Questionnaire. If the pre-Assessment result meets the criteria of the Scheme, Holistic

IT formally Assess the Questionnaire and report the result of the Assessment to the Client. Provided that the Assessment result meets the criteria of the Scheme, Holistic IT will issue a Scheme Certificate.

If the pre-Assessment fails to meet the Scheme criteria, the Client may submit up to two further Self Assessment Questionnaires for pre-Assessment within six months of the Commencement Date; if after the third pre-Assessment the responses to the Questionnaire do not meet the Scheme criteria, this Agreement will terminate.

If the formal Assessment fails to meet the Scheme's criteria, one further Self Assessment Questionnaire may be submitted for Assessment subject to the provisions of sub-clauses 8.3 and 9.2.

If as a result of any pre-Assessment or Assessment, technical assistance is required by the Client (that is, regarding making changes to the Client's systems or processes), such is not covered under the terms of this Agreement; however Holistic IT will in response to specific requests by the Client provide such technical assistance and such will be chargeable at Holistic IT's prevailing rate.

2. Assessment Levels

2.1 Cyber Essentials

Cyber Essentials is the basic Cyber Essentials accreditation, being based on self assessment verified by Holistic IT. The Cyber Essentials accreditation demonstrates that the Client has addressed the basic and essential cyber controls that a typical expert authority would expect to see in place in the smaller company. Cyber Essentials focuses on:

- Boundary firewalls and internet gateways – these are devices designed to prevent unauthorised access to or from private networks, but good setup of these devices either in hardware or software form is important for them to be fully effective
- Secure configuration – ensuring that systems are configured in the most secure way for the needs of the organisation
- Access control – Ensuring only those who should have access to systems to have access and at the appropriate level.
- Malware protection – ensuring that Malware protection is installed and is it up to date
- Patch management – ensuring the latest supported version of applications is used and all the necessary patches supplied by the vendor been applied

2.1.1 Holistic IT's Cyber Essentials Assessment can be delivered using any of the following Assistance Levels:

- Independent Certification
- Independent and Checked Certification

2.1.2 Cyber Essentials accreditation renewal must be carried out every twelve months and requires completion of the Self Assessment Questionnaire.

2.2 Cyber Essentials Plus

The Cyber Essentials Plus accreditation includes all of the requirements of Cyber Essentials and in addition:

- Within three months of the completion of the Self Assessment Questionnaire, an Audit of the systems that are in-scope for Cyber Essentials. This includes a representative set of user devices, all internet gateways and all servers with services accessible to unauthenticated internet users. Holistic IT will test a suitable random sample of these systems (typically around 10 per cent) to

confirm compliance with the responses made to the Self Assessment Questionnaire and then make a decision whether further testing is required

- A Vulnerability Test

2.2.1 Cyber Essentials Plus accreditation renewal must be carried out every twelve months and requires completion of the Self Assessment Questionnaire and an Audit.

2.2.2 Holistic IT's Cyber Essentials Plus Assessment can be delivered using any of the following Assistance Levels:

- Independent Certification
- Independent and Checked Certification

2.3 IASME Governance and GDPR

IASME Governance is the basic IASME Governance accreditation, being based on self assessment verified by Holistic IT. The IASME Governance and GDPR accreditation includes all of the requirements of Cyber Essentials and in addition:

- Risk assessment and management
- Data protection
- Policies
- Physical security
- Vulnerability management
- Training and managing people
- Change management
- Monitoring
- Backup
- Incident response and business continuity

2.3.1 Holistic IT's IASME Governance and GDPR Assessment can be delivered using any of the following Assistance Levels:

- Independent Certification
- Independent and Checked Certification

2.3.2 IASME Governance and GDPR accreditation renewal must be carried out every twelve months and requires completion of the Self Assessment Questionnaire.

3. Contact

Holistic IT's security assessment team may be contacted at any time during the Assessment on 01302 235 050 during Working Hours.