

Supplementary terms for the supply of Security Services

The Services set out in these Supplementary Terms shall be supplied by DEITG to the Client on the terms and conditions set out in DEITG's General Terms and Conditions and the terms and conditions of these Supplementary Terms. All definitions set out in the General Terms and Conditions shall, unless otherwise specified below, have the same meaning when used in these Supplementary Terms.

1. SUPPLEMENTARY DEFINITIONS

- 1.1 'Accreditation Period' means the period of validity following a successful Assessment.
- 1.2 'Assess', 'Assessment' means the assessment, by DEITG, of the Client's Security Profile against the Scheme.
- 1.3 'Assessment Services' means the provision of Assessments by DEITG.
- 1.4 'Audit' means DEITG's checking of a sample of the Client's IT systems, devices, processes and policies to verify the Client's responses to the Questionnaire.
- 1.5 'Security as a Service' means DEITG's recurring security update and advice service, as described in the Service Schedule.
- 1.6 'Security Services' means Assessment Services and Security as a Service.
- 1.7 'Security Profile' means the Client's cyber security posture / stance at the time of DEITG's Assessment.
- 1.8 'Self Assessment Questionnaire', 'Questionnaire' means the questionnaire used for the assessment of the Client's compliance with the Scheme.
- 1.9 'Site' means the Client- owned or occupied location(s) as set out in the Order, at or to which DEITG shall carry out or otherwise supply the Assessment Services.
- 1.10 'Vulnerability Test' means an automatic or manual check of the Client's systems configuration pertaining to cyber security which is performed by DEITG.

2. TERM

- 2.1 This Agreement will be effective from the Commencement Date set out on the Order.
- 2.2 If the Agreement is for the supply of Assessment Services without Security as a Service, the Agreement shall run until terminated in accordance with the terms clause 11 of the General Terms and Conditions or clause 9 hereof.
- 2.3 If the Agreement is for the supply of Assessment Services with Security as a Service, the Agreement shall run for an initial term of one year and thereafter for further for one year terms until terminated in accordance with the terms clause 11 of the General Terms and Conditions or clause 9 hereof.

3. BACKGROUND

- 3.1 The Cyber Essentials Scheme and the IASME Governance Scheme (collectively, the 'Scheme') is owned by HM Government (the 'Authority') and the IASME Consortium Ltd respectively. Its delivery is overseen by a number of contractors, the IASME Consortium Ltd (the 'Accreditation Body') being one of those. DEITG has been approved by the Accreditation Body for delivery of the Scheme.
- 3.2 DEITG's Assessment Services comprise delivery of 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, DEITG 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 DEITG 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 annually, the requirements for which are described in the Service Schedule.

4. PROVISION OF SERVICES

The Assessment Services to be supplied under the terms of this Agreement are provided either as a single Assessment or as an annually recurring Security as a Service. Both types of Assessment Service 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;
 - 4.1.4 IASME Governance (Gold) and GDPR Audited.
- 4.2 DEITG's Assistance Levels are:
- 4.2.1 Self-Certification;
 - 4.2.2 Guided Certification;
 - 4.2.3 Managed Certification.
- 4.3 Some Certification Level / Assistance Level combinations are mutually exclusive.
- 4.4 Security as a Service includes training, reporting, phishing simulations and IT security advice, as described in the Service Schedule.

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 DEITG 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 DEITG.
- 5.4 Acknowledge and agree that any Scheme Certificate shall only be issued by DEITG when DEITG, 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 DEITG.
- 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 Self Assessment Questionnaire within three months of the Commencement Date.
- 5.9 Within ten Working Days of any request for an appointment made by DEITG 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 DEITG the necessary administration credentials to allow it to carry out the test.
- 5.11 Notify DEITG immediately and in any event with not less than two Working Days beforehand if the Client wishes to cancel a previously made appointment.
- 5.12 Pay all agreed additional Charges reasonably levied by DEITG.
- 5.13 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 DEITG under the terms of this Agreement.

- 5.14 Not make any derogatory statements about the Scheme or behave in any manner that could damage the reputation of the Scheme.

6. DEITG'S OBLIGATIONS

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

- 6.1 On commencement of this Agreement, make available to the Client the Self Assessment Questionnaire.
- 6.2 Provide to 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 DEITG'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 Tests as appropriate to the level of Assessment to be conducted.
- 6.6 Carry out on-site Audit which shall be conducted and assessed at DEITG's sole discretion.
- 6.7 Carry out Vulnerability Tests at the agreed date and time, which shall be conducted and assessed at DEITG'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 DEITG'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, DEITG 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 DEITG) within six months of the Commencement Date; and
 - 6.8.3 Whilst DEITG shall not charge the Client for carrying out parts of the additional Assessment that it can execute remotely, DEITG 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 DEITG 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 If set out on the Order, provide Security as a Service for the duration of this Agreement.
- 6.11 Perform the assessment of the Self Assessment Questionnaire, any on-site Audits and Vulnerability Tests using Good Industry Practice.
- 6.12 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 DEITG has not warranted or represented the Scheme or certification there under as conferring any additional benefit to the Client.
- 8.2 If, following a failed Assessment, the Client requests assistance or other consultancy, DEITG shall provide such, chargeable at its prevailing rates.

- 8.3 If an appointment is made with the Client for a visit to Site and that at the appointed time DEITG 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, DEITG shall be entitled to charge the Client at its prevailing rate.

9. TERMINATION

- 9.1 If, as set out on the Order, the Agreement is for the supply of an Assessment without Security as a Service, the Agreement shall terminate:
- 9.1.1 On the delivery by DEITG of the Scheme Certificate following the Assessment meeting the Scheme criteria; or
 - 9.1.2 Twelve months after the Commencement Date, unless otherwise agreed in writing by DEITG, whichever event occurs earlier; or
 - 9.1.3 At any time by the Client providing written notice, whereupon all outstanding Charges shall become immediately due for payment.
- 9.2 If the Agreement is for the supply of an Assessment with Security as a Service, the Agreement may be terminated by either party providing the other not less than ninety days to terminate at the end of the Minimum Term or any Additional Term thereafter.
- 9.3 This Agreement may be terminated forthwith by DEITG if, in DEITG's reasonable opinion, the Client is in breach of sub-clauses 5.1 to 5.3 hereof.

10. CHARGES AND PAYMENT

- 10.1 The Charges for the Assessment Services shall be paid in accordance with the Order and in any case in advance of the supply of the Scheme Certificate or upon termination otherwise of the Assessment Services, whether completed or not, whichever occurs earlier.
- 10.2 If the Client terminates the Agreement for the supply of Security as a Service prior to the end of the Minimum Term or any Additional Term, the Client shall pay, by way of liquidated damages, all Charges that are due up to the end of the current term.
- 10.3 DEITG shall, not less than ninety days prior to the end of the Minimum Term or any Additional Term thereafter, notify the Client of changes to Charges and any other changes to the terms of this Agreement.
- 10.4 For the avoidance of doubt, the Charges for Security as a Service do not include the Charges for Assessment Services.

11. EXCLUSION OF LIABILITY

- 11.1 The Client agrees that DEITG 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 the Data Protection Legislation or any other data protection regulations that are 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 Tests carried out by DEITG 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 DEITG's Vulnerability Tests have been carried out and any necessary reconfiguration and any associated costs shall be the Client's sole responsibility;
 - 11.2.3 Whilst DEITG warrants that it shall use reasonable care during the execution of Vulnerability Tests, DEITG shall not be liable for any losses or damage which arise either directly or indirectly from its access to the Client's IT systems.
- 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 DEITG. The actual Assessment Services to be provided under the terms of this Agreement are listed on the Order.

1. Assistance Levels

1.1 Self Certification

Under its Self Certification Assistance Level, DEITG will provide the Client with access to the Self Assessment Questionnaire, which the Client will complete without any further assistance from DEITG. On completion of the Self Assessment Questionnaire by the Client, DEITG 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, DEITG will issue a Scheme Certificate. If an Assessment fails to meet the Scheme's criteria, the Client may submit one further Self Assessment Questionnaire for Assessment within six months of the Commencement Date. If further technical assistance is required (that is, regarding making changes to the Client's systems or processes), such is not covered under the terms of this Agreement, however DEITG in response to specific requests by the Client provide such technical assistance; such technical assistance will be chargeable at DEITG's prevailing rates.

1.2 Guided Certification

Under its Guided Certification Assistance Level, DEITG will provide the Client with access to the Self Assessment Questionnaire, which the Client will complete without any further assistance from DEITG. On completion of the Self Assessment Questionnaire by the Client, DEITG will review the completed Self Assessment Questionnaire and discuss the results with the Client, prior to formal Assessment. DEITG will offer advice and guidance (up to a maximum of two hours consultancy) on the Client's responses to the Self Assessment Questionnaire which either individually or as part of a set would cause the Assessment to fail. If further technical assistance is required (that is, regarding making changes to the Client's systems or processes), such is not covered under the terms of this Agreement, however DEITG will, in response to specific requests by the Client provide such technical assistance; such technical assistance will be chargeable at DEITG's prevailing rates. If necessary, the Client will resubmit the Self Assessment Questionnaire prior to formal Assessment. DEITG will carry out a formal Assessment of 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, DEITG will issue a Scheme Certificate. If an Assessment fails to meet the Scheme's criteria, the Client may submit one further Self Assessment Questionnaire for Assessment within six months of the Commencement Date and subject to the terms of sub-clause 6.8.3. Any time spent by DEITG providing advice and guidance on the Client's responses to the Self Assessment Questionnaire in excess of two hours will be charged at DEITG's prevailing rate.

1.3 Managed Certification

Under its Managed Certification Assistance Level, DEITG will provide the Client with access to the Self Assessment Questionnaire, which the Client will complete with question by question assistance from DEITG. DEITG will assess the Client's proposed response to each question and will offer advice and guidance thereupon. If further technical assistance is required (that is, regarding making changes to the Client's systems or processes), such is not covered under the terms of this Agreement, however DEITG will provide such technical assistance, chargeable at its prevailing rates. The Client will submit the Self Assessment Questionnaire, DEITG 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, DEITG will issue a Scheme Certificate. If an Assessment fails to meet the Scheme's criteria, the Client may submit one further Self Assessment Questionnaire within six months of the Commencement Date for Assessment and subject to the terms of sub-clause 6.8.3.

2. Assessment Levels

2.1 Cyber Essentials

Cyber Essentials is the basic Cyber Essentials accreditation, being based on self assessment verified by DEITG. 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 DEITG's Cyber Essentials Assessment can be delivered using any of the following Assistance Levels:

- Self Certification
- Assisted Certification
- Managed 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. DEITG 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.

2.3 IASME Governance and GDPR

IASME Governance is the basic IASME Governance accreditation, being based on self assessment verified by DEITG. 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
- Fault response and business continuity

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

- Self Certification
- Assisted Certification
- Managed 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.

2.4 IASME Governance and GDPR Audited

The IASME Governance and GDPR Audited accreditation includes all of the requirements of the IASME Governance and GDPR accreditation, and in addition:

- An Audit of a sample of the Client's IT Systems estate (including mobile devices), to confirm compliance with the responses made to the Self Assessment Questionnaire
- An Audit of the Client's processes and policies

2.4.1 DEITG's IASME Governance and GDPR Audited Assessment can be delivered using any of the following Assistance Levels:

- Managed Certification

2.4.2 IASME Governance and GDPR Audited accreditation renewal must be carried out every twelve months and requires completion of the Self Assessment Questionnaire annually and an Audit once every three years.

2.4.3 The Accreditation Body will moderate the Assessment.

3. Security as a Service

3.1 Security as a Service comprises an annual service under which the DEITG will provide a fixed set of services, which is charged annually with pricing based on the number of End Users and software licence costs. The Service comprises:

- Annual software renewal licences for security monitoring / simulation software
- An annual cyber training presentation to the Client's staff
- Access to online cyber training materials for all staff
- Online cyber training on staff induction
- Weekly staff phishing simulations
- Regular IT security bulletins and tips
- Quarterly security update reports
- Annual cyber board report

3.2 With the objective of mitigating new security risks, as new threats emerge DEITG will advise the Client of such and will if requested and at additional charge carry out upgrades and changes to the Client's IT infrastructure.

4. Contact

4.1 The Client shall contact DEITG's security team by one of the following methods (or as otherwise notified):

- By Email to DEITG's Service Desk: support@deitg.com

- By Telephone to the Service Desk: +353 (0)21 242 9417
- Via DEITG's website www.deitg.com/get-support

4.2 The Client may contact DEITG during the hours of 8.30am to 5.30pm Monday to Friday, excluding bank and public holidays.

5. Complaints Handling

5.1 If dissatisfied with any Security Services-related matter, the Client should make a complaint using the following escalation path. If the complaint remains unresolved, the Client should escalate to the next level in the escalation path.

Escalation Level	Role	Contact Details
1	Service Desk	+353 (0)21 242 9417
2	Service Desk Team Manager	+353 (0)21 242 9417
3	Managing Director	+353 (0)21 242 9417

5.2 Formal complaints can be made by e-mail or telephone, and will be responded to within three Working Days.