

These Consolidated Terms and Conditions ("Terms") apply to all professional services ("Services") provided by:

Mitigate Cyber Ltd, a company incorporated in England with registration number 08314901 and with its registered offices at The Old Tannery, Eastgate, Accrington, Lancashire, United Kingdom, BB5 6PW (the "**Company**"); and

Any organisation wishing to receive the Services of the Company (the "**Client**").

Company will provide the Services to Client under the Terms and a Service Contract Agreement stating the Services provided ("**SCA**").

The Terms and the SCA together will form a binding agreement between Company and Client (the "**Agreement**") under which the Services will be provided.

For the avoidance of doubt, Section A of the Terms shall apply to all Services, and Section B onwards shall apply to the specific Services to be provided and as stated in the SCA.

A. GENERAL TERMS

A.1 Engagement

The Client engages the Company and the Company shall act for the Client on the terms of the Agreement.

A.2 Term

The Company's performance of the Services as stated in each SCA ("Project") shall commence on the Agreed Start Date and continue (subject to the terms of this Agreement) until completion of the planned work ("Agreed Completion Date"). The Agreement comes into effect at the time and on the date that the final signature to the Agreement is provided. The Agreement shall end on completion of the Project and invoices related to the Project have been settled.

A.3 Duties

The Company shall complete the Project, which can be carried out either at the Client's offices or remotely or at such other location(s) as may be stated in each SCA or agreed between the parties from time to time.

A.4 Fees

- 4.1 In consideration of the Services, the Company shall invoice the Client, and the Client shall pay the Company in accordance with each SCA.
- 4.2 Any fees that remain unpaid after their due date (as stated in each related invoice), will carry an interest of 8% above HSBC Bank base rate as specified from time to time, and the Client will be liable for any additional reasonable costs that may be necessary to collect the Agreed Fee.
- 4.3 Unless the Agreed Fee is stated as being inclusive of expenses, the Company shall be reimbursed in full by the Client in respect of all expenses properly and reasonably incurred by it in connection with the Project, subject to the production of such receipts as the Client may require, attached to an invoice for the whole amount of the expenses.

- 4.4 Cancellations - The Company reserves the right to charge in full for booked consultant days where the Client cancels those consultant days with less than five business days' notice, and to charge 50% of the contracted rate where the day is cancelled between five and ten days in advance. In each case, the Company may waive the right to charge for a specific cancellation if the Company is able to deploy the Consultant's time with an alternative Client. The Company also reserves the right to charge (at cost) for any non-refundable expenses incurred in respect of travel and accommodation arrangements made in line with this agreement for any consultancy days that are cancelled, irrespective of the notice period. Cancellations in respect of training courses or other services are covered in the respective service-specific terms later in this Agreement.
- 4.5 Where the Agreed Fee in a multi-year agreement has been calculated on the basis of an unchanged scope of service from year to year, and the Client needs for any reason to increase the scope, then the Company will re-calculate the Agreed Fee on the basis of that increase in scope still taking into account the agreed multi-year discount. The Company will invoice the Client on the basis that the re-calculated fee is the new Agreed Fee and the Client will pay any invoices arising on the terms set out in this Agreement.

A.5 Liability

- 5.1 The Company shall accept no liability whatsoever in respect of any losses incurred by the Client in respect of the Company's performance under the Agreement and which arise in any way from circumstances beyond the Company's control ("force majeure" or "Acts of Nature").
- 5.2 The extent of the parties' liability under or in connection with the Agreement (regardless of whether such liability arises in tort, contract or in any other way and whether or not caused by negligence or misrepresentation) shall be as set out in this clause 5.
- 5.3 Subject to clauses 5.6 and 5.7, the Supplier's total liability shall not exceed the 100% of the value of each Contract from which a claim arises.
- 5.4 Subject to clauses 5.6 and 5.7, the Supplier shall not be liable for consequential, indirect or special losses.
- 5.5 Subject to clauses 5.6 and 5.7, the Supplier shall not be liable for any of the following (whether direct or indirect):
- i. loss of profit;
 - ii. loss or corruption of data;
 - iii. loss of use;
 - iv. loss of production;
 - v. loss of contract;
 - vi. loss of opportunity;
 - vii. loss of savings, discount or rebate (whether actual or anticipated);
 - viii. harm to reputation or loss of goodwill.

- 5.6 The limitations of liability set out in clauses 5.2 to 5.5 shall not apply in respect of any indemnities given by either party under each Agreement.
- 5.7 Notwithstanding any other provision of the Agreement, the liability of the parties shall not be limited in any way in respect of the following:
- i. death or personal injury caused by negligence;
 - ii. fraud or fraudulent misrepresentation;
 - iii. any breach of clauses 5.8 (subject to 5.8.1), A8 and A13.
 - iii. any other losses which cannot be excluded or limited by applicable law.
- 5.8 Intellectual property
- 5.8.1 Company shall indemnify the Client from and against any losses, damages, liability, costs and expenses (including reasonable professional fees) incurred by it as a result of any action, demand or claim that use of the Deliverables infringes the Intellectual Property Rights of any third party (IPR Claim), provided that Company shall have no such liability if the Client:
- a. does not notify the Company in writing setting out full details of any intellectual property rights claim (IPR Claim) of which it has notice as soon as is reasonably possible;
 - b. makes any admission of liability or agrees any settlement or compromise of the relevant IPR Claim without the prior written consent of the Company;
 - c. does not let the Company, at its request and own expense, have the conduct of or settle all negotiations and litigation arising from the IPR Claim at its sole discretion;
 - d. does not take all reasonable steps to minimise the losses that may be incurred by it or by any third party as a result of the IPR Claim;
 - e. does not, at the Company's request, provide the Supplier with all reasonable assistance in relation to the IPR Claim (at the Customer's expense) including the provision of prompt access to any relevant premises, officers, employees, contractors or agents of the Customer.
- 5.8.2 If any IPR Claim is made or is reasonably likely to be made, Company may, at its option:
- f. procures for the Client the right to continue receiving the benefit of the relevant Services; or
 - g. modify or replace the infringing part of the Deliverables so as to avoid the infringement or alleged infringement, provided the Deliverables remain in material conformance to their Specification.
- 5.8.3 The Company's obligations under clause 5.8 shall not apply to Services modified or used by the Customer other than in accordance with the Agreement and/or the Company's instructions.
- 5.8.4 The Client shall indemnify Company against all losses, damages, liability, costs and expenses (including reasonable legal fees) incurred by the Company in connection with any claim arising from such modification or use.

A.6 Non-solicitation

The Client and the Company hereby undertake to each other that for the period of 12 months following termination of the Agreement neither of them will either directly or by an agent or otherwise and whether for himself or for the benefit of any other person induce or endeavour to induce any officer or employee of the other to leave his or her employment or an associate or contractor of any sort to breach the terms of his or her contract with the Client or the Company as the case may be.

A.7 Termination

- 7.1 The Client shall be entitled to terminate the Agreement with immediate effect and without any payment in lieu of notice by giving notice in writing to the Company if the Company commits any material or persistent breach of any of the terms or conditions of the Agreement or wilfully neglects or refuses to carry out any of the duties.
- 7.2 The Company shall be entitled to terminate this Agreement immediately if the Client fails to pay any sum due within 30 days of the date of submission of an invoice properly submitted in line with the terms of the Agreement.
- 7.3 Upon termination of the Agreement, the Company shall not represent itself as being engaged by or connected with the Client or any subsidiary company.
- 7.4 If, for any reason, the Client terminates the Agreement in advance of the Agreed Completion Date, the Client agrees to pay by way of early termination fee the difference between any discounted prices included in the Agreement and the Company's published list price for those products or services at the point they were delivered.

A.8 Confidentiality

- 8.1 "Confidential" means the information pertaining to either the Company or the Client, which is communicated in confidence between the Company and the Client that is not in or has not entered the public domain and is not generally available to the public;

"Confidential Information" means all information which may be imparted or in any way made available in confidence or be of a confidential nature relating to the business or prospective business, current or projected plans or internal affairs of either the Company or the Client and in particular but not limited to all Computer Know-how, Commercial Know-how, trade secrets, unpublished information relating to any of the Company's or the Client's intellectual property and any other confidential commercial, financial or technical information relating to the business or prospective business of the Company or the Client or to any customer or potential customer, associate or potential associate or supplier or potential supplier, officer or employee of the Company or the Client or to any member or person interested in the share capital of the Company or the Client and any such information of a third party which the Company or the Client is obligated to keep confidential.

"Commercial Know-how" means all confidential information, other than Computer Know-how, relating either to the Company or the Client and the prospects,

markets, marketing, sales, finance, pricing, customers, distribution, suppliers, employees, consultants and policies of the Company or the Client.

“Computer Know-how” means all confidential information relating to the Company or the Client not at present in the public domain (including information contained in or arising from research, designs, flow charts, expressions, methodology, logic flows, specifications, drawings, manuals, lists and instructions in whatever form held) relating to computer hardware and software or that content including:

- (a) operating and applications software, including graphics, windows and hypermedia;
- (b) menu structures, macro facilities, programming languages and tools, software interfaces, and source code;
- (c) the design, development, selection, procurement, construction, installation, use, repair, service or maintenance of any software;
- (d) the Company's or Client's current or future range of software of any description;
- (e) the supply or storage of computer software or components thereof;
- (f) quality control, testing or certification; and
- (g) any media assets including but not limited to video, text, audio material, photographs, graphics, animation, artwork, scripts, story boards, treatments, synopses and any other preparatory and development materials.

8.2 The Company will not either during the period of the Agreement (other than in the proper course of its duties and for the benefit of the Client) or after the Agreement has ended for any reason whatsoever:

- (a) use, disclose or communicate to any person any Confidential Information which it will have come to know, or have received or obtained at any time (before or after the date of the Agreement) by reason of or in connection with the Agreement with the Client; or
- (b) copy or reproduce in any form or by or on any media or device or allow others to copy or reproduce Confidential Information whether or not in documentary form ("Documents") containing or referring to Confidential Information.

8.3 The Client shall, and shall procure that all its directors, officers, employees, partners and associates shall keep secret and confidential at all times all information relating to the tools, processes and methods used by the Company in the course of the Project, and agrees that these tools, processes and methods are subject to the laws of copyright and are owned by or licenced to the Company, and that they may not be copied, shared, forwarded or in any way made available to any other party save during the period of the Agreement and for the express purposes of completion of the Project.

A.9 Co-marketing and External Communications

9.1 Not Used.

9.2 Not Used.

A.10 Notices

10.1 Any notice required or permitted to be given or served under the Agreement shall be in writing and may be served by either party by personal service or by post addressed to the other party's registered office for the time being.

10.2 Any such notice shall be deemed to have been served, if delivered, at the time of delivery; or, if posted, at the expiry of 48 hours after posting.

A.11 Waivers and Remedies

11.1 The rights of each party under the Agreement may be exercised as often as necessary, and are cumulative and not exclusive of its rights under the general law.

11.2 No waiver of any of the provisions of the Agreement shall be effective unless it is expressly stated to be such in writing and signed by both parties.

11.3 Any delay in the exercise or non-exercise of any right is not a waiver of that right.

11.4 Any remedy or right conferred upon the parties for breach of the Agreement shall be in addition to and without prejudice to all other rights and remedies available to it.

A.12 Independent Contractors

The Company and the Client are independent contractors and neither shall hold itself out to be, nor shall anything in the Agreement be construed to constitute either party as the agent, representative, employee, partner or joint venture of the other. Neither party may bind or obligate the other without the other party's prior written consent.

A.13 Data Protection

13.1 Where the Company has a legitimate interest, in the context of the Agreement, in processing the personal data of the Client's employees, associates, suppliers, customers and/or partners, it will do so as a Joint Controller with the Client. The Company will retain personal data in line with its contractual, statutory or accounting obligations as set out from time to time in its retention policy.

13.2 The Client agrees that it is solely responsible for informing its employees, associates, suppliers, customers and/or partners that their personal data is being shared with the Company. The Client agrees that, in respect of this data, it will act as the point of initiation for any data subject access request ("DSAR") and the Company undertakes to provide reasonable assistance to the Client in responding to any DSAR. The Company agrees that, in respect of any Data Breach in relation to personal data shared under this clause, it will be responsible for liaising where necessary with the supervisory authorities.

13.3 The Company will protect personal data in line with its obligations under the Data Protection Act 2018 and the General Data Protection Regulation or any regulation that will supersede them.

13.4 The Company will not:

- (a) Transfer any Client personal data (or personal data relating to customers of the Client) outside the EEA other than to a country in respect of which there is a current adequacy finding by the European Commission;
- (b) Use any Client personal data (or personal data relating to customers of the Client) for marketing purposes.

A.14 Severability

If any provision of the Agreement is held invalid, illegal or unenforceable in any jurisdiction, such provision shall be severed and the remainder of the provisions of the Agreement shall continue in full force and effect as if the Agreement had been executed with the illegal or unenforceable provision eliminated.

A.15 Representations

The Company warrants and represents to the Client that it is under no obligation, covenant or restriction which would or might operate to prevent or restrict the Company from performing the obligations under the Agreement, or which may give rise to any conflict of interest between the Company and the Client or any subsidiary company of the Client.

A.16 Entire Agreement

The Agreement (which for the avoidance of doubt includes the Agreement, these Consolidated Terms and Conditions and any applicable service-specific terms and conditions) constitutes the entire understanding and agreement between the parties relating to the subject matter of the Agreement and supersedes any previous agreement between the parties.

A.17 Governing Law and Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of England and Wales without application of conflicts of laws that would otherwise apply the substantive law of any other jurisdiction, and the parties submit to the exclusive jurisdiction of the English courts.

A.18 Certification Success Guarantee

Where the objective of the Project is to prepare the Client for an independent, accredited certification audit of its standard(s)-based management system, the Company guarantees that, provided the Client has executed any business improvements identified by the Company during the Project as necessary, the Client will achieve certification and the Company undertakes to remedy or otherwise resolve at its own cost any major nonconformity raised at the initial certification audit conducted by an accredited certification body.

B. PCI DSS CONSULTANCY AND QSA SERVICES (MITICOMPLY): SPECIFIC TERMS

- B.1 The Terms in this section B are in addition to the General Terms and apply only to Agreements that cover the provision of consultancy or Qualified Security Assessor ("QSA") services in respect of the Payment Card Industry Data Security Standard ("PCI DSS").
- B.2 The Company will only conduct assessments to determine a Client's compliance with the PCI DSS in line with the QSA Validation Requirements and the PCI DSS Security Audit Procedures as made available from time to time by the Payment Card Industry Security Standards Council ("PCI SSC").
- B.3 Any Report on Compliance ("RoC") that we may make will contain an attestation that we have carried out the PCI DSS Security Audit Procedures without deviation, and that at the time of audit we did not identify any conditions of non-compliance with the PCI DSS other than those noted in the RoC.
- B.4 The Client agrees that the Company may disclose any RoC, Attestation of Compliance and other related information to the PCI SSC and/or to relevant financial institutions, acquiring banks and to relevant government, regulatory and law enforcement bodies.
- B.5 If, for any reason, the Company's appointment as a QSA is terminated, the Company may, on giving 15 days' prior written notice, terminate any aspect of the Agreement that is related to the provision of QSA services.
- B.6 Further Limitation of Liability: In addition to the limitations contained in Clause A.5 above and its subclauses, the Company accepts no liability for any information security breaches, or theft or compromise of cardholder data, or any other breach of the Client's cardholder data environment that arises from matters that were not directly and clearly disclosed to the Company during the course of its engagement, and/or that in any way arise from changes, whether to the cardholder data environment or in the cardholder security environment generally, which arise after completion of that phase of the Company's work during which we might have been in a position to identify the specific issue if the Company had been given adequate information.

**C. PENETRATION TESTING AND VULNERABILITY SCANNING (MITIHACK):
SPECIFIC TERMS**

- C.1 The Terms in this section C are in addition to the General Terms and apply only to Agreements that cover the provision of penetration testing, vulnerability assessment or social engineering services.
- C.2 Penetration testing, vulnerability assessments and social engineering services will be limited to conducting an agreed set of tests on the devices, systems, infrastructure, applications and/or sites that are identified under the heading Statement of Work within the Agreement.
- C.3 The Company's penetration testing methodology is in line with the guidance of OSSTMM and OWASP and testing is a combination of automated and manual testing, with manual testing designed to exploit any vulnerabilities identified by the automated testing. All tests look for exploitable vulnerabilities within the identified scope. Penetration tests do not include a review of the actual code of any website applications.
- C.3 All other tests and systems are out of scope and will not be tested without a signed amendment to the Agreement.
- C.4 Test IP Address: The Company's testing is carried out from a dedicated penetration testing network, and the Company will supply the Client with the relevant IP address so that the Client can add it to any IPS/IDS or filtering system to allow testing to be completed. Log files may record ping sweeps and port sweeps from the Company's test IP address in addition to other activity that may be suspicious to any SEM or SIEM deployed on the systems and applications under test.
- C.5 The Company's testers will take care not to cause Denial of Service (DOS) conditions or anything that would affect the performance of the systems under test, except where permitted by and agreed with the Client.
- C.6 The Company's testers will take care not to perform testing that will result in breaking any of the devices they identify nor will they attempt to exploit any vulnerability where they think that doing so may cause damage, nor will they intentionally damage any information or information systems during testing.
- C.7 The Company's testers will immediately report any critical risk vulnerability that they might identify to the Client contact.
- C.8 The Company will require explicit authorisation to proceed from the Client and from any additional parties involved in hosting the infrastructure or application that is in scope before the start of any test work.
- C.9 Logs are kept of the actions taken during a test and, in line with the Company's data retention procedure, these are retained, along with all other Client files, for six years and are then destroyed. Client files will be encrypted, classified as restricted to the testing consultant and to senior management of Mitigate Cyber, stored on a restricted network drive, and will be backed up in their encrypted form to the Company's mirrored, secure off-site backup environment. Within the overall context of the Mitigate Cyber ISO27001 certification, these controls directly protect the Client's data from disclosure, damage and information leakage.

- C.10 The Company will not:
- (a) disclose test results or related information to third parties without the Client's prior permission, unless otherwise required by law;
 - (b) allow anyone, other than on a need-to-know basis, access to the Client's test information;
 - (c) exchange information in relation to the tests and test results other than by using encrypted email.
- C.11 The Client will identify and disclose to the Company any third parties that may conceivably be affected by the Company's testing activities in relation to this Project, and any damages and/or loss of service caused by the Client's failure to identify and/or disclose such third parties shall remain the sole responsibility of the Client and the Client therefore indemnifies the Company against all and any costs or damages howsoever arising from such activities. The Client's authorisation to commence testing activities is deemed to include confirmation that any relevant Client-internal or external parties have been appropriately notified and that all necessary permissions from such parties for the Company to commence testing have been provided to the Company.
- C.12 The Company will only identify vulnerabilities that are already known at the date on which any tests are carried out, and which are capable of being exposed by the range of testing tools deployed by the Company. The Client accepts that it is in the nature of technical security testing that there may be flaws that will be uncovered in the future or by the use of alternative tools and attack methodologies, none of which could normally be identified at the time of testing, and therefore agrees that it will not, now or in the future, hold the Company to account for any such matters.
- C.13 The Company shall accept no liability for damages caused to the Client by any automated or non-automated attacks on the Client's internet-facing infrastructure or its applications, irrespective of whether or not the Company's security testing activity carried out under this Agreement did, did not, or could have but did not, identify any vulnerability exploited or which might in future be exploited by any such attack.
- C.14 The Company will identify vulnerabilities that its testing has exposed; wherever possible, it will identify by reference to commonly available and published information the appropriate patches and fixes that are recommended to deal with the identified vulnerability but it will be entirely the Client's responsibility to formally identify and deploy an appropriate solution to the vulnerabilities identified by the Company's security testing.
- C.15 The Company will not use any third-party consultants for carrying out any of the services under this part of an Agreement.

D. IN-HOUSE TRAINING: SPECIFIC TERMS

- D.1 The Terms in this section D are in addition to the General Terms and apply only to Agreements that cover the provision of in-house training services.
- D.2 Prices for in-house training courses include the trainer's time and all the necessary training materials. The costs for travel, accommodation, exam fees, delegate certificates and any other out-of-pocket expenses are either included in the course fee (which will therefore be described as "inclusive") or will be identified as additional costs (in which case the course fee will be described as "course fee only") and, in either case, this will be clearly set out in the Agreement.
- D.3 The Client agrees to provide:
- (a) a venue that is appropriate for the number of people attending;
 - (b) a PowerPoint projector and screen;
 - (c) two flip charts with pens; and
 - (d) tea, coffee and lunch for the delegates and the Company's trainer.
- D.6 Cancellation terms apply once the Company has accepted a booking from the Client for delivery of a training course.
- D.7 Places on in-house training courses cannot be sold on to other organisations, unless this has been specifically agreed by the Company in advance in writing.

D.8 Cancellation Charges

- D.8.1 The Client may cancel a booking without penalty providing the Company receives written notice of cancellation more than 28 business days prior to the Agreed Start Date for the relevant training course; the Client will however be liable for the cost of any travel or accommodation arrangements that have already been made by the Company and which are non-refundable.
- D.8.2 Written cancellations received by the Company between 28 and 21 business days prior to the start of the training course will be subject to a 25% cancellation fee;
- D.8.3 Written cancellations received by the Company between 20 and 11 business days prior to the start of the training course will be subject to a 50% cancellation fee.
- D.8.4 Written cancellations received ten business or fewer before the start of a training course will incur a 100% cancellation penalty; in other words, the full, agreed fee for the course will still be payable.
- D.8.5 The Company reserves the right to postpone a course without penalty if circumstances beyond the Company's control make this necessary.
- D.8.6 The Company reserves the right to cancel the training course but will endeavour not to do so within ten business days of the start of the course. If a training course is cancelled, the Company's only obligation to the Client will be, at the Company's discretion, either to reschedule the cancelled course within four months or to refund in full the fees paid by the Client for the training course.
- D.8.7 In addition to the limitation of liability terms in A.5 above, the Company will not be liable to the Client in contract, tort, negligence or otherwise for any loss, damage,

costs or expenses of any nature whatsoever incurred or suffered by the Client of a direct, indirect, special or consequential nature arising from such a cancellation.

D.9 Additional Delegates

D.9.1 The training course will be agreed at the time of booking for a maximum number of delegates. If the Client wishes to exceed this number, this must be agreed in advance and in writing with the Company, and additional fees/course costs may have to be paid in advance of the course taking place.

D.9.2 If additional, unscheduled delegates attend on the day, the Company will levy an additional charge of 20% of the course fee per additional delegate.

D.10 Delegate Background

D.10.1 The Client is responsible for ensuring that the backgrounds of its delegates is suitable for the training course they are attending. The Company will not be liable for any refund if delegates decide that the course material is inappropriate for them or if they are unable to participate fully for any reason.

D.10.2 The Client will ensure that all delegates have additional time set aside in relation to any pre-course reading material that may be provided in relation to the course they are attending, depending on its topic and duration.

D.11 Copyright and Intellectual Property

In addition to the restrictions contained in A.8 above, the Client agrees that all copyright and other intellectual property rights in or relating to any course materials provided by or made available by the Company in connection with the course are and remain the sole property of the Company and/or the Company's training partners. Course materials may not be used, copied, reproduced, stored in a retrieval system, distributed or transmitted in whole or in part or in any form or by any means, whether electronically, mechanically, or otherwise, or translated into any language, without the Company's prior written permission (which may in some cases be dependent on permission from the Company's training partners).

E. CYBER ESSENTIALS (MITICERT): SPECIFIC TERMS

- E.1 The Terms in this section E are in addition to the General Terms and apply only to Agreements that cover the provision of Cyber Essentials certification assessment and related scanning services. Clients should also read and accept the terms contained in Section C on Penetration Testing for Cyber Essentials certification services.
- E.2 The Client is required to complete any required testing and submit the completed Cyber Essentials Questionnaire ("CEQ") within 120 days of purchasing the relevant Cyber Essentials certification service. Unless there are exceptional circumstances, any applications not completed within that period will be marked as void; in these circumstances, the Client agrees that they will not be entitled to any refund of or reduction in the Agreed Fee.
- E.3 The Client is required to ensure that all vulnerability scans have been completed and submitted on the in-scope systems and infrastructure no later than seven calendar days from submitting the Cyber Essentials questionnaire to the Company. Failure to do so will result in a "fail" outcome and a new application will be required to reinstate the certification process before a positive outcome can be assessed.
- E.4 The testing methodology for Cyber Essentials and Cyber Essentials Plus will be in accordance with the requirements set out by CREST. Refer to terms related to Penetration Testing services in section C.
- E.5 All other tests and systems are out of scope and will not be tested without a signed Cyber Essentials Questionnaire.
- E.6 The Company will inform the Client where further tests are required due to a "fail" outcome of the assessment, or in the event that the questionnaire does not meet the scope. These tests will be subject to agreement with the Client, and will be billed separately.
- E.7 Explicit authorisation is required from the Client and from any additional parties involved in hosting any infrastructure or application that is in-scope before the start of any tests and should be submitted with the signed Cyber Essentials Questionnaire. This is also applicable for an online submission via the CyberComply portal.
- E.8 Limitations on the testing, such as a requirement for out-of-hours testing or weekend testing, or restrictions such as testing only during office hours should be stipulated at the time of submitting an order for Cyber Essentials certification assessment. Any surcharges incurred by the Company for any out-of-hours testing will be agreed with the Client in advance and billed separately.
- E.9 The Company's testers are all qualified to the level that CREST deems appropriate for carrying out assessments.
- E.10 Unless otherwise agreed, the Company reserves the right to list the Client's company name on its website upon achieving certification.

F. STAFF AWARENESS E-LEARNING MODULES (MITILEARN): SPECIFIC TERMS

- F.1 The terms in this section F are in addition to the General Terms and apply only to Agreements that cover the provision of staff awareness e-learning training.
- F.2 The Company owns the copyright in all the content material (whether text, graphics, designs, guidance notes, or information of any kind) contained within the Courseware, as well as in any upgrades or updates of any sort that may, from time to time, be made available to the Client.
- F.3 The Company will license a maximum number of Client users to access one or more identified e-learning courses (the "Courseware") and/or it will license a maximum number of Client users to access Courseware hosted in an e-learning portal (the "Portal") provided by the Company, all insofar as specified and described in the Agreement.
- F.4 If so specified in the Statement of Work, the Company will, as (and if) specified in the Agreement, provide a single session of training for one or more administrators nominated by the Client (the "Training") to enable the Client to administer the Portal.
- F.5 If so specified in the Statement of Work, the Company will offer the Client:
- 5.1 basic Customisation of the Portal using the Client's corporate branding;
 - 5.2 basic Customisation of the Courseware, limited to company logos and references, and links to appropriate Client policies.
- F.6 The Client's licence to access the Courseware and/or the Portal shall commence on the date of signature of the Agreement and shall continue (subject to the terms of this Agreement) until the Agreed Completion Date.
- F.7 The duties of the Company shall be, as described in the Agreement, to complete the Customisation, to provide the Training, and to provide access to or copies of the Courseware as required by the Courseware Licence and/or to provide access to the Portal, for the duration of the Agreement.
- F.8 For the purchase of the service 'Mitilearn Academy' you are entitled to a 14 day cooling off period which means if you change your mind you can cancel and receive a full refund. The 14 days starts the day after you entered into the contract for the service.
- F.9 If the e-learning module(s) is hosted on the Mitigate Cyber Hub the client agrees on the following:

F.9.1 Browsers

The Company's e-learning portals are tested as being accessible to learners whose computers use the identified versions of the following browsers:

- (a) Microsoft Internet Explorer versions 9 or later
- (b) Apple Safari v6 or later
- (c) Mozilla Firefox v25 or later
- (d) Google Chrome v30 or later

F.9.2 Cookies

The portal uses cookies to enable Client learners to carry out e-learning. By using this site, the Client agrees that the Company can place cookies on Client learners' computers.

F.9.3 Portal Uptime

Portal Uptime is the total time in a calendar month that the Portal is available on the Internet to deliver e-learning. It is the Client's responsibility to establish connectivity to the Portal. The Company takes responsibility for Portal availability; however, the Company cannot be held liable for Internet problems that occur outside of its control. With the exception of Internet outages and Scheduled Downtime, the Company guarantees that the Portal will be available to Clients for 99.5% of each calendar month.

F.9.4 Scheduled Downtime

Scheduled Downtime is any planned or schedule interruption of services from the Portal, for the purpose of Portal or infrastructure upgrades, software patching, software improvement, or for the replacement of any hardware or software, in order to provide the Client with better services. The Company will provide the Client with email notification of scheduled downtime at a minimum of 72 hours' notice. Scheduled downtime may also include periods of regular downtime, which are used for system maintenance. Details of such regular, scheduled downtime are notified separately.

F.9.5 Backups

The Company will make backups, once per day, of all data on the Portal. The Company will retain these backups for no longer than 60 days. The Company will provide an electronic copy of the backup to the Client upon written (email) request by an officer of the Client organisation. There may be an additional charge if the Client asks the Company to do this more than once per year. The Company does not keep regular snapshots of progress through courses by individual Client learners, and the Company will not necessarily keep backups of all reports that the Client might create for itself within the Portal.

F.9.6 Information and Data Security

The Company takes what it considers to be reasonable steps to prevent unauthorised access to the Portal, and to the Client's data stored on the Portal. In particular, the Company takes appropriate steps to protect all personal data that is stored on the Portal. These steps include ensuring that the Portal is securely configured, that vulnerabilities are dealt with as identified, that updates and patches are applied when they are released, that passwords are encrypted, and that access rights are appropriately managed. The Client and the Company acknowledge that, for the purposes of the Data Protection Act 1998, the Client is the Data Controller and the Company is the Data Processor of any Client data received in the provision of the services. The Company shall process the Client's data only to the extent, and in such a manner, as is necessary for the purposes of providing the services to the Client as described in this Agreement. The Company shall only process the Client's data in accordance with the Client's instructions from time to time and not for any other purpose. The Company will process personal data within the EEA. The Company shall implement appropriate technical measures to protect Client data (including all personal data) against any unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might

result from any unauthorised or unlawful processing, accidental loss, destruction or damage to the 'Client's data having regard to its nature.

The Client agrees that it will ensure that its users are instructed in the use of the Portal and any Courseware, and the Company reserves the right to delete or otherwise block access to the Portal by any of the Client's users who are, or the Company reasonably suspects may be, engaged in any activity that might breach international or UK law or which may in any way affect the performance of the Portal or its continued use by the Client's users.

G. DPO-AS-A-SERVICE (MITICOMPLY): SPECIFIC TERMS

G.1 The terms in this section G are in addition to the General Terms and apply only to Agreements that cover the provision of data protection officer (“DPO”) services.

G.2 Scope of Work

G.2.1 DPO-as-a-service will be limited to providing the specific DPO services (“the Services”) that are identified under the heading Statement of Work in the Agreement.

G.2.2 The Company shall not be responsible for any failure to advise or comment on any matter that falls outside the scope of the Services as described in the Agreement.

G.2.3 The Services are provided solely for the Client’s benefit and any specific advice provided in relation to any specific issue or matter within the scope of the Services is restricted to that issue. It may not be used or relied on for any other purposes or by any person other than the Client without the Company’s prior written agreement.

G.2.4 The Client recognises and understands that the Company is not licensed to provide legal services, that the Company does not present itself as providing legal advice, and that any advice given by the Company in the course of providing the Services is not legal advice.

G.2.5 The Client agrees that it will be solely responsible for obtaining appropriate legal advice on any matters on which it needs legal advice and that it will be solely responsible for agreeing and settling any legal fees arising in respect of that advice.

G.2.6 The Company relies on the Client to ensure that all directors and authorised officers of the Client fully understand these Terms and Conditions and that any instructions or questions from such directors, officers any other individuals are authorised by the Client on the terms set out here.

G.2.7 The Client agrees to provide the Company with appropriate resources and access to relevant data and processes in order for the Company to provide the Services.

G.2.8 The Client shall make available a Board Member to whom the Company can report in respect of the Services.

G.3 Liability

G.3.1 This section is subject to and in addition to the terms set out in Section A.5

G.3.2 The Client agrees that Client alone is responsible for its compliance with the GDPR and any other relevant laws and regulations, not limited to those relating to personal data.

G.3.3 The Client agrees that the Services are provided by the Company, and not by any employees of the Company, and that the liability of the Company in respect of the services is limited to the Company. The Client agrees that it will under no circumstances seek to bring any form of action, legal or otherwise, against any employee of the Company in relation to the Services.

- G.3.4 The Company shall not be liable for any delay in providing advice or guidance within the scope of the Services where this is caused by circumstances beyond our reasonable control.
- G.3.5 The Company shall not be liable for failure or delay in performance by the Client in respect of advice, guidance or instructions given within the scope of the Services where due to causes beyond our reasonable control. Where the Services require the Company to deal with third parties on behalf of the Client, we do not accept any liability in relation to such third parties.
- G.3.5 If there are other advisers or third parties involved in any matter on which the Company is also engaged, the extent to which any loss or damage will be recoverable by the Client from the Company will be limited, without prejudice, in proportion to the overall fault for such loss or damage or as agreed in advance with the other parties. If the Company's ability to claim a contribution to its costs under these circumstances from a third party is prejudiced by any limitation of liability agreed by the Client with that third party, the Company shall not be liable to the Client for any amount that the Company would have been able to recover from that third party but for that limitation of liability.
- G.3.6 In respect of obtaining advice on any issue that is within scope of the Services, it is the responsibility of the Client to engage with the Company in a timely manner. The Company shall not be held liable for any delay in the Client engaging the Services and any associated delay in the Company delivering the Services.
- G.3.7 It is the responsibility of the Client to follow the advice provided by the Company within the scope of the Services. Should the Client not follow the advice provided by the Company, the Company shall not be held liable for any consequences, financial or otherwise, experienced by the Client as a result. If the Client fails to follow any advice provided by the Company within the scope of the Services, the Company shall be entitled to terminate this Agreement with immediate effect and without any obligation to make any refund of any fees already paid under the Agreement
- G.3.8 Unless otherwise agreed in writing the Company is not responsible for reminding the Client of key dates or other time-sensitive actions or information.

G.4 People responsible for delivering on behalf of the Company

- G.4.1 The Company undertakes to ensure that those of its employees who are deployed to provide the Services have the necessary skills, knowledge and experience. The Client agrees that the Company alone will determine what skills, knowledge and experience are necessary in relation to the Services.
- G.4.2 The Services will be carried out by a team of employees of the Company and the contact details for the team will be provided in the Agreement.
- G.4.3 The Company will identify a lead manager within the DPO team who has ultimate responsibility within the Company for delivery of the Services to the Client. If the Company changes the lead manager for any reason the Company will notify the Client as quickly as possible.

G.5 Processes and Procedures

G.5.1 GDPR advice & guidance, including helpline

- G.5.1.1 The Company will provide email and telephone advice only to nominated contacts of the Client, such nominations to be made in writing.
- G.5.1.2 A request for advice or guidance will be recorded, assessed and allocated a priority level in accordance with the Companies Assessment Criteria detailed in Section G.7 and passed to the most appropriate GDPR consultant to respond in line with the Company's Resolution Times as detailed in Section G.8.
- G.5.1.3 Following assessment of the priority level, the Company will send the Client an email acknowledgement detailing the priority level, expected resolution time and details of the allocated GDPR consultant.
- G.5.1.4 The Company will record and track all requests for advice or guidance or other types of calls received by the Client, including: date; time; caller; subject matter; response time; and resolution time. A quarterly report will be generated by the Company and sent to the nominated contacts at the Client. This report will also record the trends in terms of the categories of requests, highlighting root causes of issues raised and potential organisational issues.

G.5.2 Review of GDPR policies

- G.5.2.1 The Client will provide the Company with copies of all its policies and procedures that relate to data protection and compliance with EU data protection legislation.
- G.5.2.2 The Company will review all documents provided in accordance with G.5.2.1 in relation to their compliance with applicable laws and regulations. The Company will provide written feedback to the Client, highlighting areas for improvement, as soon as possible.

G.5.3 GDPR e-learning modules

- G.5.3.1 The terms set out in Clause F apply.

G.5.4 GDPR audit

- G.5.4.1 The Company will allocate appropriate consultants to carry out GDPR audits as required for the Services.
- G.5.4.2 Audits will be scoped, planned and executed in line with relevant audit planning guidelines. Those who perform audits will not be from the same team that is providing the advice being audited.
- G.5.4.3 Audit reports, with recommendations for improvement or otherwise, will be provided to the client after completing the data gathering phase of the audit and after undergoing any necessary further review.

G.5.5 GDPR updates

- G.5.5.1 The Company will provide the Client's nominated contacts with regular updates on issues critical to data protection compliance.

G.5.5.2 The copyright in all the updates (whether text, graphics, designs, guidance notes, or information of any kind) may belong to the Company or to other third parties.

G.5.5.3 The Client may distribute internally to the Client any update material to which the Company owns the copyright but is hereby notified that any third party material may have different copyright restrictions and that the Client is solely responsible for complying with any restrictions in respect of such third party material.

G.6 Availability of Services

G.6.1 The Services will be provided between the hours of 09:00am and 17:00pm Monday to Friday, except bank holidays.

G.6.1.1 Calls received outside of the standard hours of service will go through to an answerphone service and will not be accessed by the Company until the next working day.

G.6.1.2 Emails received outside of the standard hours of service will be received by the Company's server but no action will be taken by the Company until the next working day.

G.6.2 The Company guarantees that the advice & guidance service will be available to Clients for 99.5% of each calendar month.

G.7 GDPR advice & guidance assessment criteria

G.7.1 All enquiries for advice or guidance will be assessed and assigned a priority level as described below using the following criteria:

1. Number of data subjects affected
2. Threat to confidentiality, integrity and availability of personal data
3. Effect on the rights and freedoms of data subjects
4. Effect on the Client's business mission
5. Context of the data processing problem
6. Deadlines
7. Estimated solution time
8. Frequency of occurrence of the problem
9. Client's guidance on priority

G.7.2 The Client will be informed by email of the priority rating and anticipated resolution time.

G.8 Resolution Times

G.8.1 Within the context established in G.6, all enquiries for advice or guidance will be allocated a maximum resolution time based on an assigned priority level, as follows:

Priority Level	Definition	Response Times
Urgent	Advice on a topic that has immediate high risks to the rights & freedoms of data subjects	Within 4 hours
Important	Advice on a topic which has potential high risks to the rights & freedoms of data subjects and / or a high impact on the Client's business objectives / deliverables	Within 24 hours
Low	Advice which has limited impact on the rights & freedoms of data subjects but has an imposed deadline	Within 3 working days
Routine	Advice which has limited or no impact on the rights & freedoms of data subjects and does not have an imposed deadline	Within 10 working days