



pentest
INFORMATION SECURITY ASSURANCE

A Shearwater Group plc
Company

Pentest Limited

Terms and Conditions

1 DEFINITIONS AND INTERPRETATION

- 1.1 “Client” means the individual(s) and/or organisation(s) to whom the Company is providing Security Testing and who has signed and completed a Penetration Test Authorisation Form and Proposal Acceptance Form;
- 1.2 “Company” means Pentest Limited (Co. Reg. No. 11925182);
- 1.3 “Conditions” means the terms and conditions set out in the Contract between Company and Client;
- 1.4 “Confidential Information” means all tangible and intangible information designated as confidential by any party in writing together with all other information which may reasonably be regarded as confidential including, but not limited to, Intellectual Property, procedures, network configuration and topology, passwords, private encryption keys and details of the Company’s methodologies and know-how, trade secrets, personal information, details of the Clients’ System, made available communicated or delivered to the recipient directly or indirectly in connection with this Contract.
- 1.5 “Consultant” means the individual(s) provided by Company for the performance of the Security Testing;
- 1.6 “Contract” includes these Terms and Conditions, the Proposal, Authorisation Form and the Proposal Acceptance Form which is entered into once an offer has been accepted pursuant to clause 3.5 of these terms and conditions;
- 1.7 “Data Protection Laws” means all applicable law relating to the processing, privacy and/or use of Personal Data, as applicable to either party or the services provided by Pentest including: (a) the GDPR; (b) the Data Protection Act 2018; (c) any laws which implement or supplement any such laws; and (d) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing;
- 1.8 “End Date” means the date the Security Testing will be completed as confirmed by the Company in the Authorisation Form.
- 1.9 The terms “**Data Controller**”, “**Data Processor**”, “**Data Subject**”, “**Personal Data**”, “**Personal Data Breach**” and “**Process/Processing**” have the same meaning as described in the Data Protection Laws
- 1.10 “Event of insolvency” means if the Client is unable to pay its debts (within the meaning of Section 123 of the Insolvency Act 1986) or becomes insolvent, or is subject to an order or a resolution for its liquidation, administration, winding-up or dissolution (otherwise than for the purposes of a solvent amalgamation or reconstruction), ceases or threatens to cease to carry on its business or has an administrative or other receiver, manager, trustee, liquidator, administrator or similar officer appointed overall or any substantial part of its assets, or enters into or proposes any composition or arrangement with its creditors generally, or is subject to any analogous event or proceeding in any applicable jurisdiction;
- 1.11 “Fees” means Company’s fees for the Security Testing as detailed in the Proposal, and all reasonable expenses incurred by the Consultant in carrying out the Security Testing which will be agreed in advance with the Client;

- 1.12 “Force Majeure” means any cause preventing either Party from performing any or all of its obligations under these Conditions which arises from or is attributable to any acts, acts of god, pandemics, events, omissions or accidents beyond the reasonable control of the Party so prevented;
- 1.13 “Good Industry Practice” means in relation to any circumstances the exercise of that degree of professionalism, skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or an internationally recognised company engaged in the same type of activity under the same or similar circumstances;
- 1.14 “Group” means any undertaking which from time to time is a parents undertaking, subsidiary undertaking and any subsidiary undertaking of any such parents undertaking where ‘parent undertaking’ and ‘subsidiary undertaking’ have the meanings given to them in section 1162 of the Companies Act 2006.
- 1.15 “Intellectual Property Rights” (IPR) means any copyright, patent, design patent, registered design and design rights, utility models, trademarks, service marks, an application for any of these or the right to supply for the same, trade secrets, know-how, database rights, moral rights, confidential information, trade or business names and any other industrial and proprietary and other similar protected rights , in each case subsisting at any time in any part of the world (whether registered or unregistered) and any: (a) pending applications or rights to apply for registrations of any of these rights that are capable of registration in any country or jurisdiction; and (b) similar or analogous rights to any of these rights in any jurisdiction;
- 1.16 “Party” means any party to, or the parties to, this Contract;
- 1.17 “Penetration Test Authorisation Form” means the Company’s form to be signed by the Client and submitted to Company when ordering the Security Testing;
- 1.18 “Proposal Acceptance Form” means the form completed by the Client which sets out the Start Date, the End Date of testing, the location and the number of days for the testing;
- 1.19 “Proposal” means the proposal for the Security Testing provided by the Company to the Client detailing the scope of work, all or some of which may be accepted by the Client. in their purchase order;
- 1.20 “Authorisation Form” means the Company’s form setting out the agreed scope of work to be signed by the Client and submitted to Company when ordering the Security Testing;
- 1.21 “Security Testing” means the process of testing the System as described in the Proposal made by the Company to the Client;
- 1.22 “Start Date” means the date the Security Testing will start to be provided as confirmed by the Company in the Authorisation Form and Proposal Acceptance Form;
- 1.23 “System” means the systems and networks which the Client requires to be security tested pursuant to this Contract;
- 1.24 “Test Report” means the report produced by the Company detailing the results of the Security Testing;
- 1.25 “VAT” means value added tax as defined under the Value Added Tax Act 1994.
- 1.26 Any statute or statutory provision includes any subordinate legislation made under the statute or statutory provision (as amended, consolidated or re-enacted) from time to

time except to the extent that any such amendment, extension or re-enactment would increase or alter the liability of a party under this Agreement.

2 APPLICATION OF CONDITIONS

- 2.1 These Terms and Conditions apply to and form part of the Contract between the Company and the Client.
- 2.2 When the Company has received a signed Proposal Acceptance Form, this constitutes an offer by the Client for Security Testing subject to these Terms and Conditions.
- 2.3 An offer may be withdrawn or amended by the Client at any time before acceptance by the Company.
- 2.4 Regardless of the date of acceptance of the offer, these Terms and Conditions shall, absent any signed Proposal Acceptance Form, be effective from the commencement of Security Testing by the Company.
- 2.5 An offer shall not be accepted, and no binding Contract to supply Security Testing shall arise, until the earlier of:
 - 2.5.1 the Company's written acceptance of the offer; or
 - 2.5.2 the Company performing the Security Testing or notifying the Client that they are ready to perform the Security Testing (as the case may be).
- 2.6 Rejection by the Company of an Offer, including any communication that may accompany such rejection, shall not constitute a counter-offer capable of acceptance by the Client.
- 2.7 The Company shall perform the Security Testing for the Client using reasonable skill and care and in a professional, timely manner.
- 2.8 The Proposal Acceptance Form will state the Start Date and End Date for the provision of the Security Testing, time not being of the essence.
- 2.9 Where a Test Report is required, it shall, unless otherwise agreed, be produced and sent to the Client by the Consultant within ten (10) working days or as agreed with the Client on completion of the Security Testing.
- 2.10 Whilst the Company will use reasonable endeavours to ensure that the same Consultant will continue throughout the Security Testing, it reserves the right to replace that Consultant if necessary, at its reasonable discretion by notifying the Client.
- 2.11 The Company shall, where the Consultant is present on the Client's premises, ensure that the Consultant complies with such reasonable site rules and procedures as are prior notified to the Company.

3 THE CLIENT AGREES

- 3.1 To obtain appropriate consent from its ISP (Internet Service Provider), only where the ISP is hosting services on behalf of the Client and any other relevant third party supplier of the System, only where the third party supplier is hosting services on behalf of the Client for the Security Testing to be carried out and, when requested by the Company, to provide evidence of such consent and to notify relevant employees that the Security Testing has been scheduled and that they may be monitored;

- 3.2 To arrange a mutually convenient time with the Company for the performance of the Security Testing and to inform its ISP of the date agreed with the Company in accordance clause 3.1;
- 3.3 To make appropriate backups of the System prior to the commencement of the Security Testing;
- 3.4 That, where the Security Testing is to take place on the Client's premises, the Client shall ensure that suitable accommodation is provided for the Consultant which shall include network access and, where necessary, access to data centres, server rooms and/or switch rooms;
- 3.5 That should the Client require a laptop or Personal Digital Assistant (PDA) to be security tested by the Company it will deliver the laptop and/or PDA to the Company's registered address and collect it from those premises or authorise other means of delivery and return at the Client's own risk. The Company shall not be liable for the laptop or PDA during transit to or from its offices;
- 3.6 The Client or such Group will compensate the Company for any direct indirect losses incurred as a result of a claim from a third party arising out of any failure of the Client or such Group to comply with clauses 3.1, 3.2 and 3.3 provided always that the Company shall mitigate any and all losses and provide written notice of any claim to the Client within 10 working days;
- 3.7 To provide the Company with at least one employee who shall have substantial computer systems, network and project management experience of the Client's Systems to act as liaison between the Client and the Company;
- 3.8 To co-operate with the Company and to provide it promptly with such information about its Systems, network, premises, equipment, data structures, protocols, software, hardware and firmware as are reasonably required by the Company;
- 3.9 To ensure that, where the Security Testing is taking place on its premises, the premises are safe;
- 3.10 That, by signing the Penetration Test Authorisation Form, the Client consents, for itself and on behalf of all Client's Group companies, to the Company performing the Security Testing and that it has procured, where necessary, the consent of all its (and its group companies) employees, agents and sub-contractors that the Company shall be permitted to carry out the Security Testing. The Company will be carrying out the Security Testing in the belief that it has all appropriate consents, permits and permissions from the Client and the Client's Group companies (and their employees, agent and sub-contractors);
- 3.11 That the Company makes no representation or warranty that the assessment will identify all possible vulnerabilities or other security threats within the target(s);
- 3.12 That while the Company executes tests with reasonable care and skill, it cannot and does not warrant that no damage or loss of availability will be sustained by the Client;
- 3.13 That, whilst the Company will conduct all Security Testing in line with Good Industry Practice and make all reasonable efforts to avoid disruption of the Client's network, the tools and techniques used may cause disruption to the Client's Systems and/or possible loss of or corruption to data and the Client agrees to take such backups and provide such redundant systems as are prudent in the circumstances. The Company will notify the

Client in the event where activity would lead to loss of service or data before proceeding where this is known to the Company;

- 3.14 To notify the Company immediately if there are any periods during Security Testing when the Company should stop work due to critical business processes (such as batch runs) or if any part of the System is business critical so that the Company can, if need be and with the Client's consent, modify its testing approach;
- 3.15 That, where the Company supplies any software as part of the Security Testing, it shall only use such software for lawful purposes or in accordance with its intended purpose;
- 3.16 That, during the performance of the Security Testing and for a period of 12 months after completion of the Security Testing, it will not recruit any employees or personnel of the Company or such Group which it met or was introduced to through its relationship under this Contract without the prior written consent of the Company or such Group;
- 3.17 Where the duration for testing is limited (**Time Limited Testing**) in accordance with the Client's allowances and upon the Client's request, the Client accepts that this will not be a complete and full test to the best of the Company's capabilities. The scope of Time Limited Testing would be agreed by the Client and Company and defined in the proposal, authorisation form and purchase order (if applicable).

4 FEES AND PAYMENT

- 4.1 Subject to 4.2 below and unless otherwise agreed, the Fees payable under this Contract shall be invoiced on delivery of the Test Report or, if none is to be provided, on completion of the Security Testing.
- 4.2 Invoices are due for payment within 30 days of the date of the invoice. All payments due under this Contract shall become due immediately upon termination of this Contract despite any other provision in this Contract. All payments due under this Contract shall be made without any deduction by way of set off, counterclaim, discount or abatement or otherwise.
- 4.3 The Company shall be entitled to interest on any payment not paid when properly due pursuant to the terms of these conditions, calculated from day to day at a rate per annum equal to 3% above the base rate of Lloyds Bank Plc and payable from the day after the date on which payment was due up to and including the date of payment (whether before or after judgment).
- 4.4 All sums under the Contract are unless otherwise stated, exclusive of VAT. Any VAT payable in respect of such sums shall be payable in addition to such sums and shall be payable in addition to such sums, at the rate from time to time prescribed by law on delivery of a valid VAT invoice.
- 4.5 The Company reserves the right to invoice the Client upon acceptance of the order an amount of 10% of the estimated Fees that will be charged for the performance of the Security Testing to cover the costs of initiating and preparing for the performance of the Security Testing ("Initial Fee"). The Initial Fee will be treated as a payment on account of the total Fees charged for the Security Testing.

5 CONFIDENTIALITY

- 5.1 Each party undertakes that it shall keep any information that is confidential in nature concerning the other party and its Affiliates including, any details of its business, affairs, customers, clients, suppliers, plans or strategy (**Confidential Information**) confidential and that it shall not use or disclose the other party's Confidential Information to any person, except as permitted by clause 5.2
- 5.2 A party may:
- 5.2.1 disclose any Confidential Information to any of its employees, officers, representatives or advisers (**Representatives**) who need to know the relevant Confidential Information for the purposes of the performance of any obligations under this Agreement, provided that such party ensures that each of its Representatives to whom Confidential Information is disclosed is aware of its confidential nature and agrees to comply with clause 5 as if it were a party;
 - 5.2.2 disclose any Confidential Information as may be required by law, any court, any governmental, regulatory or supervisory authority (including any securities exchange) or any other authority of competent jurisdiction provided that such party shall provide notice as promptly as practicable to the other party of its obligation to make any disclosure required by law ; and
 - 5.2.3 except as permitted under clause 5.2.2, use Confidential Information only to perform any obligations under this Agreement.
- 5.3 Each party recognises that any breach or threatened breach of clause 5 may cause irreparable harm for which damages may not be an adequate remedy. Accordingly, in addition to any other remedies and damages, the parties agree that the non-defaulting party may be entitled to the remedies of specific performance, injunction and other equitable relief without proof of special damages.
- 5.4 The provisions of this clause 5 shall not apply to:
- 5.4.1 subject to clause 5.6, any information which was in the public domain at the date of the Contract;
 - 5.4.2 subject to clause 5.6, any information which comes into the public domain subsequently other than as a consequence of any breach of the Contract or any related agreement; and
 - 5.4.3 subject to clause 5.6, any information which was or is independently developed by a party without using information supplied by a party or by any Affiliate of a party.
- 5.5 Clause 5 shall bind the parties during the Term and for a period of three years following termination of this Agreement.
- 5.6 To the extent any Confidential Information is Personal Data such Confidential Information may be disclosed or used only to the extent such disclosure or use is in compliance with and does not conflict with the provisions of clause 10.

- 5.7 Upon the termination or expiration of this Agreement or upon the Client's request, Company shall destroy or erase permanently (on all forms of recordation) any Client Confidential Information including Personal Data in Company's possession and confirm in writing to Client that it has done so.

6 INTELLECTUAL PROPERTY RIGHT

- 6.1 Ownership of all Intellectual Property Rights in the System remains at all times with the Client and/or its ISP or other third-party supplier. For the avoidance of doubt, all Intellectual Property Rights in the materials used by the Company to carry out the Security Testing remain vested in the Company or any relevant third-party owners.
- 6.2 All Intellectual Property Rights in the results of the testing shall belong to the Client.
- 6.3 Copyright in the Test Report shall remain with the Company, but the Client is hereby granted a non-exclusive, non-transferable licence to copy and use the Test Report for its own internal purposes only. The Client cannot send any Test Report to a third party without the prior written consent of the Company.
- 6.4 The Client undertakes to not forward the Test Report or any copies or reproductions of it to any penetration testing company or entity.

7 LIABILITY

- 7.1 Nothing in this clause 7 excludes or limits the liability of the Company for fraudulent misrepresentation or for death or personal injury caused by the Company's negligence. Save as aforesaid the following provisions set out the entire financial liability of the Company (including any liability for the acts or omissions of its employees, agents and sub-contractors) to the Client, its ISP or any third party supplier of the System to the Client.
- 7.2 The Company shall not be liable for any loss, damage, costs, expenses or other claims for compensation arising from any materials, requirements or specifications provided by the Client or instructions supplied by the Client which are incomplete, incorrect, inaccurate, illegible or defective in any other way. The Company should highlight to the Client any known errors if possible.
- 7.3 The Company shall not be liable for any loss or damage caused to either the Client, its ISP or other third party supplier of the System either jointly or severally except to the extent that such loss or damage is caused by the negligent acts or omissions of or a breach of any contractual duty by the Company, its employees, agents or sub-contractors in performing the Security Testing.
- 7.4 The Company's or such Group total liability in respect of all claims arising under or by virtue of this Contract or in connection with the performance of this Contract shall not exceed 200% in aggregate of the charges set out in the purchase order prior to a claim being made.
- 7.5 The Company and the Client and such Groups shall not be liable to each other for any of the following loss or damage (whether indirect, indirect or consequential): (i) loss of

profit; (ii) loss of business; (iii) interruption of business; (iv) loss of data; (v) loss of use; (vi) depletion of goodwill; (vii) loss of contract; (viii) loss or corruption of software or systems; (ix) loss of production, whatsoever or howsoever caused under this Agreement whether in tort (including negligence), contract or other legal theory even if such loss was reasonably foreseeable.

8 TERMINATION CANCELLATION DELAYS

- 8.1 The Company reserves the right to withdraw from the Security Testing by providing up to 5 working days' written notice, if, in its reasonable opinion, information required for satisfactory completion of the Security Testing and requested by the Company in writing is either not provided or, if provided, is inaccurate or inadequate. The Client shall be liable for any fees and expenses incurred up to and including the date of withdrawal.
- 8.2 The Company reserves the right to cancel Security Testing pursuant to clause 8.1 or to re-schedule the Security Testing. Cancellation or Rescheduling by the Client will incur the following additional fees:
 - 8.2.1.1 Cancellation or re-scheduling with at least 11 working days' written notice prior to Security Testing will incur no charge.
 - 8.2.1.2 Cancellation or re-scheduling with written notice given between 6 and 10 working days prior to Security Testing will incur a charge of 50% of the Fees.
 - 8.2.1.3 Cancellation or re-scheduling with written notice given within 5 or fewer working days prior to Security Testing will incur a charge of 100% of the Fees.
 - 8.2.2 If the Security Testing is re-scheduled, the Company will request email confirmation from the Client stating they want to book the test and require either specific dates or a time frame (e.g, before a certain date), as well as the names of the testers.
- 8.3 Subject to clause 8.1, any delays to the Start Date caused by the Client's failure to provide a suitable testing environment, deliver the required credentials, or satisfying all defined pre-requisites will be subject to a payment by the Client for any additional days needed to complete the Security Testing. These additional days will be charged at the full daily rate. This clause specifically addresses delays due to the Client's non-compliance with pre-requisites and does not apply to cancellations or rescheduling as described in clause 8.2.
- 8.4 Where the Start Date is delayed for the reasons set out in clause 8.1, and only where available, Time Limited Security Testing may be provided to the Client but will be subject to payment by the client of the full price quoted for the full duration plus an additional charge to be determined by the Company for providing additional resources to meet the End Date.
- 8.5 The Company reserves the right to collect a deposit of 25% of the Fees, which will be applied toward any applicable cancellation charges specified above.

9 EXCLUSION OF THIRD-PARTY RIGHTS

- 9.1 A person who is not a party to this Contract shall not have any rights under the Contract (Rights of Third Parties) Act 1999 to enforce any term of this Contract.

10 DATA PROTECTION

- 10.1 Each party agrees that, in the performance of their respective obligations under this Agreement, it shall comply with the provisions of Schedule 1.

11 FORCE MAJEURE

- 11.1 Neither party to the Contract shall be deemed to be in breach of these conditions or otherwise liable to the other party in any manner whatsoever for any failure or delay in performing its obligations to the extent that the same is caused by Force Majeure. In the event the Force Majeure continues for a continuous period in excess of thirty (30) working days, either party shall be entitled to give notice in writing to the other party.
- 11.2 If either party is unable to perform its duties and obligations under this agreement as a result of a Force Majeure Event, that party will give written notice to the other of the inability stating the reason in question. The operation of this agreement including clause 9.2 will be suspended during the period (and only during the period) during which the Force Majeure Event continues.
- 11.3 Immediately upon the Force Majeure Event ceasing to exist, the party relying upon it will give written notice to the other of this fact.
- 11.4 In the event the Force Majeure continues for a continuous period in excess of ninety (90) working days and substantially affects the commercial basis of this agreement, the party not claiming relief under this clause 12 will have the right to terminate this agreement upon giving 14 days written notice of such termination to the other party.

12 GENERAL

- 12.1 Any amendments or supplements to the Contract shall only be valid if agreed to by the parties in writing.
- 12.2 The Consultant shall have no authority to amend the terms and conditions of this Contract or to relieve the Client of any of its obligations under these conditions or to increase the Company's obligations under these conditions or waive any of the Company's rights under these terms and conditions. The Consultant shall have no authority to incur expenditure in the name of or an account of the Company or hold themselves out as having authority to bind the Company.
- 12.3 The Company does not give any warranty or undertaking or make any representation (either express or implied) as to the completeness or accuracy of any information provided to the Client prior to this Contract which relates to or is provided in respect of these terms and conditions by or on behalf of the Company.

-
- 12.4 These standard terms and conditions together with the Penetration Test Authorisation Form and the Proposal, shall constitute the entire agreement between the Parties and supersede any previous agreement or understanding and may not be varied except in writing between the Parties and signed by their respective authorised signatories. All other terms and conditions express or implied by statute or otherwise, are excluded to the fullest extent permitted by law. As regards Security Testing, in the event of any conflict or ambiguity between any of the terms of these documents the following order shall prevail:
- (1) Penetration Test Authorisation Form;
 - (2) Proposal Acceptance Form
 - (3) The terms and conditions in this Contract; and
 - (4) Proposal.
- 12.5 Any notice sent under this Contract shall be in writing addressed to the other Party at its registered office or principal place of business or such other address as may be notified by each Party to the other time to time.
- 12.6 No failure or delay by either party in exercising any of its rights under this Contract shall be deemed to be a waiver of that right.
- 12.7 If any provision or any part of a provision of this Contract is held by any authority to be invalid and unenforceable, the validity of the other provisions and/or the remaining part of the provision shall not be affected.
- 12.8 This Contract shall be governed by the laws of England and the Parties submit to the exclusive jurisdiction of the English courts, except for enforcement proceedings where the English courts shall have non-exclusive jurisdiction.

SCHEDULE 1

DATA PROTECTION

Part A Operative provisions

1 Definitions

1.1 In this schedule:

Controller	has the meaning given in applicable Data Protection Laws from time to time;
Data Protection Laws	means, as binding on either party or the Services: (a) the GDPR; (b) the Data Protection Act 2018; (c) any laws which implement or supplement any such laws; and (d) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing;
Data Subject	has the meaning given in applicable Data Protection Laws from time to time;
GDPR	means the General Data Protection Regulation, Regulation (EU) 2016/679, as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time);
International Organisation	has the meaning given in applicable Data Protection Laws from time to time;
Personal Data	has the meaning given in applicable Data Protection Laws from time to time;
Personal Data Breach	has the meaning given in applicable Data Protection Laws from time to time;

processing	has the meaning given in applicable Data Protection Laws from time to time (and related expressions, including process , processed and processes shall be construed accordingly);
Processor	has the meaning given in applicable Data Protection Laws from time to time;
Protected Data	means Personal Data received from or on behalf of the Client in connection with the performance of the Company's obligations under this Agreement; and
Sub-Processor	means any agent, subcontractor or other third party (excluding its employees) engaged by the Company for carrying out any processing activities on behalf of the Client in respect of the Protected Data.

2 Client's compliance with data protection laws

The parties agree that the Client is a Controller and that the Company is a Processor for the purposes of processing Protected Data pursuant to this Agreement. The Client shall at all times comply with all Data Protection Laws in connection with the processing of Protected Data. The Client shall ensure all instructions given by it to the Company in respect of Protected Data (including the terms of this Agreement) shall at all times be in accordance with all Data Protection Laws. Nothing in this Agreement relieves the Client of any responsibilities or liabilities under any Data Protection Laws.

3 Company's compliance with data protection laws

The Company shall process Protected Data in compliance with the obligations placed on it under Data Protection Laws and the terms of this Agreement.

4 Instructions

4.1 The Company shall only process (and shall ensure Company Personnel only process) the Protected Data in accordance with Part B of this Schedule 1 and this Agreement (including when making any transfer to which paragraph 8 relates), except to the extent:

- 4.1.1 that alternative processing instructions are agreed between the parties in writing; or
- 4.1.2 otherwise required by applicable law (and shall inform the Client of that legal requirement before processing, unless applicable law prevents it doing so on important grounds of public interest).

4.2 Without prejudice to paragraph 2 of this Part A, if the Company believes that any instruction received by it from the Client is likely to infringe the Data Protection Laws it shall be entitled to cease to provide the relevant Services until the parties have agreed appropriate amended instructions which are not infringing.

5 Security

Taking into account the state of technical development and the nature of processing, the Company shall implement and maintain the technical and organisational measures set out in Part B of this Schedule 1 to protect the Protected Data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access.

6 Sub-processing and personnel

6.1 The Company shall:

- 6.1.1 not permit any processing of Protected Data by any agent, subcontractor or other third party (except its or its Sub-Processors' own employees in the course of their employment that are subject to an enforceable obligation of confidence with regards to the Protected Data) without the prior specific written authorisation of the Client;
- 6.1.2 prior to any Sub-Processor carrying out any processing activities in respect of the Protected Data, appoint such Sub-Processor under a written contract containing materially the same obligations as under this clause **Error! Reference source not found.**1 (including those relating to sufficient guarantees to implement appropriate technical and organisational measures) that is enforceable by the Company and ensure such Sub-Processor complies with all such obligations;
- 6.1.3 remain fully liable to the Client under this Agreement for all the acts and omissions of each Sub-Processor as if they were its own; and
- 6.1.4 ensure that all persons authorised by the Company or any Sub-Processor to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential.

7 Assistance

- 7.1 The Company shall (at the Client's cost) assist the Client in ensuring compliance with the Client's obligations pursuant to Articles 32 to 36 of the GDPR (and any similar obligations under applicable Data Protection Laws) taking into account the nature of the processing and the information available to the Company.
- 7.2 The Company shall (at the Client's cost and expense) taking into account the nature of the processing, assist the Client (by appropriate technical and organisational measures), insofar as this is possible, for the fulfilment of the Client's obligations to respond to requests for exercising the Data Subjects' rights under Chapter III of the GDPR (and any similar obligations under applicable Data Protection Laws) in respect of any Protected Data.

8 International transfers

The Company shall not process and/or transfer, or otherwise directly or indirectly disclose, any Protected Data in or to any country or territory outside the *United Kingdom* or to any International Organisation without the prior written authorisation of the Client, except where required by applicable law (in which case the provisions of paragraph 4.1 of this Schedule 1 shall apply).

9 Audits and processing

The Company shall, in accordance with Data Protection Laws, make available to the Client such information that is in its possession or control as is necessary to demonstrate the Company's compliance with the obligations placed on it under this Schedule 1 and to demonstrate compliance with the obligations on each party imposed by Article 28 of the GDPR (and under any equivalent Data Protection Laws equivalent to that Article 28), and allow for and contribute to audits, including inspections, by the Client (or another auditor mandated by the Client) for this purpose (subject to a maximum of *one* audit request in any 12 month period under this paragraph 9). The Company shall, however, be entitled to withhold *information where it is commercially sensitive or confidential to it or its other customers*.

10 Deletion/return and survival

On the end of the provision of the Services relating to the processing of Protected Data, at the Client's cost and the Client's option, the Company shall either return all of the Protected Data to the Client or securely dispose of the Protected Data (and thereafter promptly delete all existing copies of it) except to the extent that any applicable law requires the Company to store such Protected Data. This Schedule 1 shall survive termination or expiry of this Agreement.

Part B

Data processing and security details

Section 1—Data processing details

Processing of the Protected Data by the Company under this **Agreement** shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in this Part B.

1 Subject-matter of processing:

Penetration Testing services

2 Duration of the processing:

During length of each client engagement and relationship only

3 Nature and purpose of the processing:

Sales and customer relationship management

4 Type of Personal Data:

Contact details of the customer representatives (i.e. email addresses, names, phone numbers)

5 Categories of Data Subjects:

No special categories

6 Specific processing instructions:

N/A

Section 2—Minimum technical and organisational security measures

- 7 The Company shall implement and maintain the following technical and organisational security measures to protect the Protected Data:
- 7.1 In accordance with the Data Protection Laws, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of the Protected Data to be carried out under or in connection with this Agreement, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons and the risks that are presented by the processing, especially from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Protected Data transmitted, stored or otherwise processed, the Company shall implement appropriate technical and organisational security measures appropriate to the risk, including as appropriate those matters mentioned in Articles 32(1)(a) to 32(1)(d) (inclusive) of the GDPR.