SAPPHIRE TECHNOLOGIES LIMITED

Schedule 1

This is Schedule 1 which is referenced in and forms part of the Contract for the supply of Security Consultancy Services between Sapphire Technologies Ltd (the "Supplier") and [CUSTOMER NAME] (the "Customer").

SECURITY CONSULTANCY SERVICES SUPPLEMENTAL TERMS AND CONDITIONS

1 GENERAL

1.1 These Supplemental Security Consultancy Services Terms and Conditions shall apply where the Supplier provides a Solution to the Customer which includes the provision of Security Consultancy Services.

1.2 These Supplemental Terms and Conditions are in addition to all rights and obligations set out in the General Terms and Conditions and are to be read in conjunction with them.

1.3 For the purpose of these Supplemental Terms and Conditions, Security Consultancy Services shall be the Services as set out in the Service Description in Schedule 2 to the General Terms and Conditions.

1.4 The definitions and the rules of interpretation set out in clause 21 of the General Terms and Conditions shall apply to these Security Consultancy Services Supplemental Terms and Conditions.

2. SECURITY CONSULTANCY SERVICES

2.1 The Customer acknowledges and agrees that the Services provided by the Supplier under this contract (or part of the Contract where other services are also provided) are consulting service only, and any and all decisions taken by the Customer, including without limitation whether or not to follow any advice provided by the Supplier (whether verbally or in writing), is solely the Customer's responsibility.

2.2 The Customer acknowledges and agrees that the effectiveness of the Services provided and the success of any actions undertaken by the Supplier in the provision of the Services are not guaranteed or warranted by the Supplier in any respect whatsoever.

2.3 Penetration Testing and Vulnerability Assessments shall only cover the listed IP Addresses and Host names the Customer provides to the Supplier and are detailed in the Cover Sheet.

2.4 If limitations on testing are not included in the Cover Sheet or Contract Change Note they are not deemed to apply.

2.5 The Customer acknowledges that

(a) the threat of malicious attacks is constantly evolving and it is recommended that the Customer regularly commissions services of the type detailed in this Contract; and

(b) any test is only an overview of a moment in time and limited to the matters set out in the Statement of Works

3. CUSTOMER OBLIGATIONS

3.1 The Customer is responsible for the accuracy of all information the Customer provides to the Supplier including in the Cover Sheet and warrants, undertakes and represents to the Supplier that it will with all due and proper care and diligence, and having regard to the nature of the Services to be provided, verify and ensure the accuracy of all such information and of the Supplier's lawful right to use it in providing the Services, in the manner detailed in this Contract.

3.2 The Customer shall ensure that its Authorised Representative is available to the Supplier at all reasonable times to co-ordinate any testing activities that form part of the Services.

3.3 The Customer shall ensure and procure that all of its personnel who are informed of any testing or other activities that form part of the Services shall keep such information strictly confidential and shall not disclosure it, to ensure the validity of the test results.

3.4 Unless specifically requested by the Customer in writing or documented in the Cover Sheet, the Supplier shall not attempt to exploit the Customers Security vulnerabilities and shall use its reasonable endeavours to prevent permanent damage to the Customer's Test Systems. The Customer acknowledges, however, that the aim of the Services is to test the Customer's cyber defences, as well as the Customer's ability to detect and respond to a range of internal and external malicious attacks and that in the course of performing the Services service interruption is possible. It is the Customer's responsibility to restore its Test Systems to a secure configuration after the Supplier has carried out the tests.

3.5 The Customer shall sign and return to the Supplier a completed Letter of Authorisation before the Supplier commences the Services, confirming that the Supplier is lawfully authorised to perform the Services on the Customer's behalf and that the Customer has and shall at all times maintain all necessary or desirable Measures in place to lawfully permit the Supplier to perform the Services without being in breach of any Applicable Law or Requirement.

3.6 Where Computer Assets, Test Systems, Customer Data or information that is to be the subject of the Services, is operated or owned by any third party, the Customer shall procure prior to the commencement of the Services that such third party signs and delivers to the Supplier a legally binding contract in like terms to the Contract, and/or such alternative and/or additional agreements as the Supplier may from time to time require.

3.7 The Customer shall make the Supplier expressly aware in advance of the performance of any relevant Services, including completing such documentation and/or providing such information as the Supplier shall require, which of the Customer's systems are critical and are to be excluded from any testing.

3.8 The Customer warrants, represents, and undertakes that:

3.8.1 it has implemented or obtained, and shall continue to maintain all Measures necessary or desirable for the Supplier to lawfully provide the Services without being in breach of any Applicable Law or Requirement;

3.8.2 its employment contracts and policies lawfully permit the Supplier to carry out the Services on the Customer's behalf, pursuant to the terms of this Contract without being in breach of any Applicable Law or Requirement;

3.8.3 it shall at all times comply with all relevant Applicable Law including Data Protection Legislation, the Human Rights Act 1998, the Computer Misuse Act 1990, the Serious Crime Act 2015, the Police and Justice Act 2006, the Terrorism Act 2000, EU Directive 2013/40/EU, the Digital Economy Act, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Investigatory Powers

Act 2016, and any other relevant and Applicable Law which relate to the provision and receipt of the Services and/or ensuring that the Supplier may lawfully perform the Services, pursuant to the terms of this Contract.

3.8.4 it authorises the Supplier to access the Customer's Computer Assets and Test Systems for the purpose of performing the Services and such access and our performance of the Services in accordance with the terms of this Contract shall be lawful and not constitute a breach of any Applicable Law.

3.8.5 all information the Customer obtains as a result of the Services will be used by the Customer lawfully and for its own internal business purposes only, in accordance with all Applicable Law and Requirements.

3.8.6 the Customer's purpose in procuring the Services is to help to prevent crime in the form of malicious attacks including cyber-attacks on its Test Systems, Customer Data and information and Security.

3.8.7 it is the legal owner and person in charge of the Computer Assets, Test Systems and the Customer Data and information stored on any media on or related to the same, all of the IP addresses it provides to the Supplier lawfully belong to the Customer and that it has the lawful right to control the operation of the Computer Assets, Test Systems, Customer Data and information which shall be the subject of the Services, where a third party router or IP address range is involved a subnet shall not overlap onto other equipment now owned by the Customer and have the express or implied consent to intercept communications transmitted by means of a public telecommunications system with lawful authority and the Customer hereby irrevocably and unconditionally consent to and authorise the Supplier to:

(a) perform the Services, and

(b) access the Computer Assets, the Test Systems and the Customer Data and information thereon,

in accordance with the terms of this Contract, to perform the Services.

3.8.8 The Customer and its personnel are not acting for purposes which are wholly or mainly outside the Customer's trade, business, craft, or profession.

3.9 The Customer acknowledges that the provision of the Services may modify, damage, or disrupt its Computer Assets and/or Test Systems and hereby authorise the Supplier to access its Computer Assets and Test Systems for the purpose of performing the Services in accordance with the terms of this Contract.

3.10 The Customer acknowledges that the act of testing may generate extensive logs on its firewall and intrusion detection system (IDS) systems and that in general such testing is designed to directly test for security vulnerabilities on specific hosts and there is no attempt made to evade detection by IDS systems. The Customer shall ensure that such systems are configured in such a way that such traffic shall not cause any performance issues and that such systems shall not interfere with such tests.

4. INTELLECTUAL PROPERTY RIGHTS

The Customer may use the Reports and copy and disclose the whole but not part of the Reports to those of its personnel, employees, officers, representatives, contractors or subcontractors, its subsidiary or holding companies and advisers who need to know the content of such Reports for the Customer's own internal lawful business purposes provided always that the Customer does

not modify, delete, or amend any content and that the Customer complies with all Applicable Law and Requirements.

5. DATA PROTECTION

The Customer agrees to indemnify the Supplier for loss of data or information caused by the activities described in this Contract. This clause 5 applies during the Contract and after it has ended.

6. LIMITATION OF LIABILITY

6.1 In addition to the provisions on limitation of liability as set out in clause 10 of the General Terms and Conditions, the Supplier excludes all liability howsoever arising:

6.1.1 as a result of any act or omission by the Customer in following or declining to follow the Supplier's advice or recommendations provided as part of the Services provided under the Contract; and

6.1.2 for decisions made with reliance upon advice provided by a Supplier consultant, subject to clause 6.2.

6.2 Subject to clause **Error! Reference source not found.**, the Supplier shall be liable any loss arising out of or in connection with any Report, only in the event of the Supplier acting in gross negligence or wilful misconduct, but not otherwise.

6.3 In the performance of the Services, the Supplier may be required to take possession of Customer property including Customer Computer Assets and any Customer Data or information thereon. The Supplier accepts such property on and subject to the following conditions:

6.3.1 The Customer shall accurately complete, sign and submit to the Supplier a record of items form, or Data Recovery request in such format as the Supplier reasonably requires from time to time, in relation to such property on the Supplier's receipt of it and on its return to the Customer.

6.3.2 The Supplier shall take such reasonable steps as it considers reasonable and appropriate in relation to the safety of such property whilst it is in its possession. However, subject to clause **Error! Reference source not found.** and without prejudice to our obligations under applicable Data Protection Legislation, ownership and risk in such property shall remain at all times with the Customer and subject to clause 6.2, and without prejudice to our obligations under applicable Data Protection Legislation, the Supplier accept no responsibility for any loss or damage to such property.

6.3.3 The Supplier shall not be liable for any claims regarding the physical functioning of any Computer Assets or the conditions or existence of Customer Data stored on any Computer Assets or media the Customer supplies to the Supplier, at any time.

6.3.4 The Customer confirms it is aware of the inherent risks of damage to media that is involved when undergoing Data Recovery processes, including, risks due to destruction or damage to the media, and/or the data or information stored and inability to recover data or information, or inaccurate or incomplete data recovery, including those that may result from the Supplier's negligence and the Customer shall assume the risk for any and all property damage that may arise as a result of the performance of Data Recovery Services by the Supplier pursuant to the terms of this Contract. In the event of any

damage or loss to any original media supplied by the Customer, the Supplier's liability shall be limited to providing the Customer with similar media of comparable capacity.

7. EXPRESS AUTHORITY AND INDEMNITIES

7.1 The Customer acknowledges and agrees that the Supplier is performing the Services at the Customer's direction and to the extent that the Services entail activities to be undertaken by the Supplier (including our personnel, officers, employees, agents, consultants and representatives) which are in contravention or breach of any Applicable Law including the Computer Misuse Act 1990, the Customer hereby irrevocably and unconditionally authorises and consent to the Supplier carrying out such activities as the Customer's authorised agent and the Customer hereby indemnifies the Supplier from and against any and all liability suffered or incurred and arising from:

7.1.1 carrying out such activities; and/or

7.1.2 that is caused by or contributed to (to the extent so contributed) any action or omission of the Customer in breach of the terms of the Contract.

7.2 In relation to any Digital Forensics Services and/or Data Recovery Services, the Supplier is engaged by the Customer to perform, the Customer hereby authorise the Supplier and its personnel to receive and transport any storage media, Computer Assets and/or data to, from and between the Customer's and the Supplier's premises, and to use data recovery processes upon the same to endeavour to recover, access and/or process data held or stored on the same.

7.3 The Customer acknowledges and agrees that during the performance of the Services the Supplier may discover material which is illegal to store, manufacture, distribute or view pursuant to Applicable Laws or Requirements including pursuant to the Protection of Children Act 1978 as amended by the Sexual Offences Act 2003 and that it is irrevocably and unconditionally authorised to deal with such material in any manner required by Applicable Law or Requirements including referring the same to the Relevant Authorities including the police and/or the Financial Conduct Authority.

This clause 7 applies during the Contract and after it has ended.

9. Delay in Commencement of Work.

9.1 In the event the Service do not commence within 45 days of receipt of a Purchase Order, and such delay is caused by the Customer's or its personnel's actions or omissions however arising, the Supplier reserves the right to requote the cost and apply an increase of up to 10% of the total agreed value of the Service as stated it the Purchase Order.

9.2 Notwithstanding any other provision of the Contract, the Customer acknowledges and agrees that the Supplier reserves the right to issue an invoice for all Services or Solutions provided under any Purchase Order pursuant to the Contract, regardless of whether such Services or Solution have been fully delivered, if 180 days have elapsed from the date of the relevant Purchase Order. The invoicing right is applicable to the total agreed value as stipulated within the Purchase Order, reflecting both completed and uncompleted portions of the Services or Solution at that time. Surcharge for Onsite working.

9.3 The Supplier may apply a surcharge of £200 per day for expenses for all Services which must be carried out from a location specified by the Customer where the work could otherwise be completed remotely.

10. Cancellations and Postponements

10.1 to the Supplier may charge for Services or Solutions cancelled or deferred as follows:

10.1.1 In full in respect of Services or Solutions cancelled or deferred within 9 Business Days of the confirmed scheduled delivery or start date; and

10.1.2 50% of the Charges, in respect of Services or Solutions cancelled or deferred between 10 and 21 Business Days of the scheduled delivery or start date.