SCHEDULE 2 SERVICE DELIVERABLES

1 Definitions

1.1 In this Agreement the following words and expressions shall have the meanings set out below:

"Attack Surface" means an attack surface is the total sum of Vulnerabilities that can be exploited to carry out a security attack. Attack surfaces can be physical or digital. Both physical and digital attack surfaces should be limited in size to protect surfaces from anonymous, public access.

"Penetration Test" means a method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might. In a Penetration Test, if a Vulnerability is identified and an exploit exists for that Vulnerability, then the exploit will be used to gain access to the target device.

"Phishing" means a type of electronic mail attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering

"Remediation" means after Vulnerabilities are identified and assessed, appropriate remediation can take place to mitigate or eliminate the Vulnerability.

"Vulnerability/ies" means the existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

"Vulnerability Assessment" means the process of identifying risks and Vulnerabilities in computer networks, systems, hardware, applications, and other parts of the IT ecosystem. Vulnerability Assessments provide security teams and other stakeholders with the information they need to analyse and prioritise risks for potential remediation in the proper context. Vulnerability Assessment stops after the Vulnerability has been identified. It does not run exploits to gain access to targets.

2 INSIGHT SECURE OVERVIEW

2.1 Maintel Insight is a suite of consultancy and discovery services that provide our customers with the intelligence they need to make informed choices about their existing technology and to aid the planning and future development of their estate.

2.2 Insight Secure assessment products are broken down into various tests and procedures using a combination of automated and manual tools and managed by our in-house Certified Threat Intelligence Analysts team. They have extensive cyber security experience and are regular participants in major cyber events. Our Security Operations team are also members of multiple professional associations and have strong connections to the cyber security industry. 2.3 Additional definitions can be found in the 'jargon buster' document found on the Insight Secure landing page HERE.

PCI DSS CONSULTANCY AND QSA SERVICES: SPECIFIC TERMS

2.4 Where the Order contains PCI DSS Services or the provision of consultancy or Qualified Security Assessor ("**QSA**") Services in respect of the Payment Card Industry Data Security Standard ("**PCI DSS**"); the Customer shall immediately enter into a PCI DSS Agreement. Where the PCI DSS Agreement is not agreed for whatever reason, Maintel shall have no liability to supply these Services.

3. PENETRATION TESTING AND VULNERABILITY ASSESSMENT: SPECIFIC TERMS

3.1 Maintel shall deliver the provision of penetration testing, vulnerability assessment or social engineering services as set out and agreed in an Order.

3.2 Penetration testing, vulnerability assessments and/or 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.

3.3 Maintel penetration testing methodology is in line with recognised standards, testing is a combination of automated and manual testing. The manual testing is designed to exploit any vulnerabilities identified by the automated testing. The tests look for exploitable vulnerabilities within the identified scope. Penetration tests do not include a review of the actual code of any website applications.

3.4 Any and all other tests and systems not identified within an Order are out of scope and will not be tested.

3.5 Test IP Address: Maintel testing is carried out from a dedicated penetration testing network, and Maintel will supply the Customer with the relevant IP address allowing the Customer to add it to any IPS/IDS or filtering system to enable testing to be completed. Log files may record ping sweeps and port sweeps from the Maintel 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.

3.6 Maintel testers will take all reasonable endeavours 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 Customer.

3.7 Maintel testers will take all reasonable care not to perform testing that will result in:

a) the breaking any of the devices they identify;

b) or the attempted exploitation of any vulnerability where they reasonably believed doing so, may cause damage.

c) or intentionally damage any known information or information systems during testing.

3.8 Maintel testers will report with haste to the Customer any critical risk vulnerability that they might identify.

3.9 Maintel will require explicit authorisation to proceed from the Customer and from any additional parties involved in hosting the infrastructure or application that is in scope before the start of any test work, such to be provided by the Customer completion of the Authority to Test document.

3.10 Logs are kept of the actions taken during a test and, in line with Maintel's (and where applicable Maintel's third parties) data retention procedure. These are retained, along with other Customer files, for six years and destroyed. Customer files will be encrypted, classified as restricted to the testing consultant and to senior management of Maintel and it's approved third parties, stored on a restricted network drive, and will be backed up in their encrypted form to a mirrored, secure off-site backup environment.

3.11 Maintel will not:

(a) disclose test results or related information to third parties without the Customer's prior permission, unless otherwise required by law;

(b) allow anyone, other than on a need-to-know basis, access to the Customer's test information;

(c) exchange information in relation to the tests and test results other than by using encrypted email.

3.12 The Customer will identify and disclose to Maintel any third parties that may conceivably be affected by Maintel testing activities in relation to this project. Any damages and/or loss of service caused by the Customer's failure to identify and/or disclose such third parties, shall remain the sole responsibility of the Customer and the Customer indemnifies Maintel against all and any costs or damages howsoever arising from such activities.

3.13 The Customer's authorisation to commence testing activities, shall be deemed to include confirmation that any relevant Customer-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 Maintel.

3.14 Maintel 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 Maintel. The Customer accepts that there may be flaws to the testing which

may be uncovered in the future or by the use of alternative tools and attack methodologies. The Customer agrees that it will not, now or in the future, hold Maintel liable in any way for any such matters.

3.15 Maintel shall accept no liability for damages caused to the Customer by any automated or non-automated attacks on the Customer's internet-facing infrastructure or its applications; irrespective of whether the Maintel security testing activity has been carried out under this Agreement and did/did not and/or could have/ but did not; identify any vulnerability exploited or which might in future be exploited by any such attack.

3.16 Maintel 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. It will be entirely the Customer's responsibility to formally identify and deploy an appropriate solution to the vulnerabilities identified by Maintel's security testing.

CANCELLATION OF EITHER THE PENETRATION TESTING AND/OR VULNERABILITY ASSESSMENT:

3.17 Maintel reserves the right to Charge in full for booked consultant days where the Customer cancels those consultant days with less than five (5) Business Days' notice, and to Charge fifty percent (50%) of the agreed rate where the day is cancelled between five (5) and ten (10) days in advance. In each case, Maintel may waive the right to Charge for a specific cancellation if the Maintel is able to deploy the consultant's time with an alternative Customer. Maintel 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. In the event that a penetration test was cancelled this clause may also be applied.

3.18 Where the agreed Charges include a multi-year agreement, such Charges are calculated on the basis of an unchanged scope of Service from year to year. In the event the Customer needs for any reason to amend the scope of Services, Maintel may re-calculate the Charges on the basis of the change. Maintel will invoice the Customer on the basis that the re-calculated fee is the new Charge and the Customer will pay any invoices arising on the terms set out in this Agreement.

4. CYBER ESSENTIALS: SPECIFIC TERMS

4.1 Maintel shall deliver the provision of Cyber Essentials certification assessment and related scanning services as set out and agreed in an Order and pursuant to paragraph 3 of this Schedule 2.

4.2 The Customer is required to complete any required testing and submit the completed Cyber Essentials Questionnaire ("**CEQ**") within one hundred and twenty (120) days of purchasing the relevant Cyber Essentials certification service. Unless there are exceptional circumstances (agreed in writing with Maintel), any applications not completed within that period will be marked as void; in these circumstances, the Customer agrees that they will not be entitled to any refund of or reduction in the Charges.

4.3 The Customer is required to ensure that all vulnerability scans have been completed and submitted on the in-scope systems and infrastructure, no later than seven (7) calendar days from submitting the CEQ to Maintel. 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.

4.4 The testing methodology for Cyber Essentials and Cyber Essentials Plus will be in accordance with the requirements set out by CREST and subject to paragraph 3 of this Schedule 2.

4.5 All other tests and systems are out of scope and will not be progressed without a signed CEQ.

4.6 Maintel will inform the Customer where further tests are required due to a "fail" outcome of the assessment, or in the event that the CEQ does not meet the required scope. These tests will be subject to agreement with the Customer and will be invoiced separately.

4.7 Explicit authorisation is required from the Customer and from any additional parties involved in hosting any infrastructure or application that is in-scope; prior to the commencement of any tests and should be submitted with the signed CEQ. This applies also where an online submission via the CyberComply portal has been completed.

4.8 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 Maintel for any out-of-hours testing will be agreed with the Customer in advance and invoiced separately.

4.9 Unless otherwise agreed, Maintel reserves the right to list the Customer's company name on its website upon achieving certification.

5. STAFF AWARENESS E-LEARNING MODULES: SPECIFIC TERMS

5.1 Maintel shall deliver the provision of staff awareness e-learning training where specifically set out and agreed in an Order.

5.2 Subject to clause 7 of this Agreement, Maintel shall own full title to the Intellectual Property Rights contained within the courseware, alongside any upgrades or updates of any sort that may, from time to time, be made available to the Customer.

5.3 Maintel will license a maximum number of Customer users to access one or more identified e-learning courses (the "**Courseware**") and/or it will license a maximum number of Customer users to access Courseware hosted in the Portal, provided by Maintel insofar as specified and described in the Agreement.

5.4 If so specified in the Order Maintel will, as (and if) specified in the Agreement, provide a single session of training for one or more administrators nominated by the Customer (the "**Training**") to enable the Customer to administer the Portal.

5.5 If so specified in the Order, Maintel will offer the Customer:

5.5.1 basic customisation of the Portal using the Customer's corporate branding;

5.5.2 basic customisation of the Courseware, limited to company logos and references, and links to appropriate Customer policies.

5.6 The Customer's licence to access the Courseware and/or the Portal shall commence on the date of signature of this Agreement and shall continue (subject to the terms of this Agreement) until termination of the Order or the Agreement.

5.7 Maintel shall complete the agreed 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 this Agreement.

5.8 In the event that the e-learning module(s) are hosted on the Maintel Portal the Customer fully agrees the following:

5.8.1 Browsers:

Mantel's Portal is 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

5.8.2 Cookies:

The Portal uses cookies to enable Customer learners to carry out e-learning. In using this site, the Customer agrees that Maintel can place cookies on the Customer learners' computers.

5.8.3 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 Customer's responsibility to establish connectivity to the Portal. Maintel takes responsibility for Portal availability; however, Maintel cannot be held liable for Internet problems that occur outside of its reasonable control. With the exception of Internet outages and scheduled downtime, Maintel agrees the Portal will be available to the Customer for 99.5% of each calendar month.

5.8.4 Scheduled Downtime:

Scheduled downtime means any planned or scheduled interruption of Services available via the Portal. It is envisaged that any such downtime shall be 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 Customer with better Services. Maintel will give the Customer no less than three

(3) days advance notice of scheduled downtime. A maintenance notification will be sent to the Customer, using the change control process.

5.8.5 Backups

Maintel will make backups, once per day, of all data on the Portal. Maintel will retain these backups for no longer than sixty (60) days. Maintel will provide an electronic copy of the backup to the Customer upon request via the Support Portal. Maintel does not keep regular snapshots of progress through courses by individual Customer users and will not necessarily keep backups of all reports that the Customer might create for itself within the Portal.

5.9 The Customer agrees that it will ensure that its users are instructed in the use of the Portal and any Courseware. Maintel reserves the right to delete or otherwise block access to the Portal by any of the Customer's users who are, or Maintel 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 Customer's users.

6 End User Support

Customer Web Portal

6.1 Customers are provided with a dedicated web portal that allows access to the Maintel Incident Management system and enables the tracking of incidents, problems and change requests. Each Incident raised receives a web reference which is unique to the Incident and confirms that the ticket has been received by the Service Desk. This reference will be used throughout the life of the ticket to track updates and the ultimate resolution of the Incident.

