1. Authority & Consent to Test

This agreement is made as of \customtext2 {"label":"Day (number), Month, Year (YYYY)"}\, by and between:

Maintel Europe Limited, 160 Blackfriars Road, Southwark, London. SE1 8EZ ("Maintel")

and,

{{OPPORTUNITY_ACCOUNT_NAME}} (Company Legal Name), located in

{{ACCOUNT_REGISTERED_ADDRESS}} (Address),

{{ACCOUNT_COUNTRY_OF_REGISTRATION}} (Country); represented by

{{OPPORTUNITY_QUOTE_CONTACT__R}} (Contact Name); hereafter referred to as "The ("Customer").

Maintel and the Customer hereby agree to the following terms and conditions regarding any necessary security tests that both parties agree are required to be performed by Maintel (which together with Annex 1, 2 & 3 shall form the "Agreement"). Where such security tests are prescribed under any another agreement and there is a conflict, the terms of this Agreement shall prevail with regards to any relevant security tests.

Any defined terms herein shall be set out in Annex 3 Definitions below:

1. Maintel will, upon reasonable written notice to the Customer perform a Vulnerability Assessment. This partially automated test will attempt to remotely identify security vulnerabilities and/or software configuration errors - on one or more public facing systems owned and/or operated by the Customer (the "Tests").
2. The details of the Customer's host IP addresses, ranges, URL or any other resources (referred as the "assessment scope") shall be given to the Customer in a Scope Worksheet within 30 days of the completion of the Tests.
3. Maintel is authorised by the Customer to perform the Tests on the dates set out in Annex 2. For the avoidance of doubt, the Tests shall not include any form of Penetration Testing.
4. Maintel and the Customer will communicate to each as required via the phone or email details set out in Annex 2.
5. At any time during the Tests, the Customer can request in writing that Maintel promptly cease the Tests.
6. Maintel warrants that it will perform the Tests in a responsible and professional manner in accordance with industry best practices and that it will use reasonable endeavours not to change, impede or amend any applications, data, programs or components of or on the Customer's network or computer systems that are directly subject to the Tests.
7. Maintel does not offer any implied or express guarantees that the results of the Tests will mean that the Customer's network is secure from every form of attack, as Cyber Security is a rapidly and continually changing field.
8. The Customer hereby unconditionally guarantees that it has the legal right to allow Maintel full access to the systems that will be accessed by Maintel pursuant to this Agreement and that if it is not the owner of the systems it has obtained such right from the legal owner of those systems.
9. The Customer will not, pursuant to this Agreement hold Maintel liable for any indirect, punitive, special, incidental, or consequential damage (including but not limited to loss of business,

revenue, profits, use, data or other economic advantage) however it arises, whether for breach or in tort, even if Maintel has been previously advised of the possibility of such damage.

10. The Customer has the sole responsibility for adequate protection and backup of data and/or equipment used in connection with the Tests and will not make any claim against Maintel for lost data, re-run time, inaccurate output, work delays or lost profits resulting from the Tests.
11. Neither party will divulge any information that has been disclosed between parties in relation to the Tests. All elements of this Agreement shall be treated as confidential and will be treated as such by both parties.
12. Confidential information can only be used for the purpose of the Tests. Where disclosure to a third party is essential, the party wishing to disclose the information shall obtain the prior written authorisation to do so from the other party.
13. All confidential material not necessary for Test Reports will be destroyed or returned immediately after the Tests have been performed. Any other confidential information will be destroyed or returned as agreed between the parties in writing.
14. The Customer hereby agrees to respond in a normal fashion when it detects the Tests in its firewall logs, alert systems, etc. as it would do in case of a genuine Security Penetration; in order not to distort the results of the Test. Furthermore, the Customer agrees not to notify any legal or public authorities or other third parties of any Security Penetration or Test carried out pursuant to this Agreement.
15. This Agreement and it's Annexes constitute the entire agreement between parties related to the Tests. No change, alterations or modifications shall be valid unless prior agreed in writing, dated and signed by both parties.

Hereby agreed by and on behalf of:

Customer

Signature	\signature1\
Print Name	\title1\
Title	\customtext1 {"label":"Job Title"}\
Date	\date1\

By and on behalf of:

Maintel Europe Limited

Signature	\signature2\
Print Name	\customtext2 {"label":"Please Full Name"}\
Title	\customtext2 {"label":"Job Title"}\
Date	\date2\

2. Annex 1 Scope Worksheet

What specific hosts, network address ranges, or applications should be tested?

Total number of external Ip addresses

Total number of internal IP addresses

How many VLANs are in scope for the test?

Are all IP address available from one physical location?

What specific hosts, network address ranges, or applications should explicitly NOT be tested?

List any third parties that own systems or networks that are in scope as well as which systems they own (written permission must have been obtained in advance by the target organisation):

Will the test be performed against a live production environment or a test environment?

Reason for testing (PCI, GDPR, ISO, New application, Test plan, annual testing / etc)

Does the scope include any systems classified under the Government Protective Marking Scheme?

Customer

Signature	\signature1\
Print Name	\title1\
Title	\customtext1 {"label":"Job Title"}\
Date	\date1\

By and on behalf of:

Maintel Europe Limited

Signature	\signature2\
Print Name	\customtext2 {"label":"Please Full Name"}\
Title	\customtext2 {"label":"Job Title"}\
Date	\date2\

3. Annex 2 Contact Details & Test Criteria

Vulnerability Assessment Team Contact Information

Maintel Contact Information:

Maintel Primary Contact:
Maintel Mobile Phone:
Maintel Secondary Contact:
Maintel Mobile Phone:

Customer Contact Information:

Customer Primary Contact:
Customer Mobile Phone:
Customer Secondary Contact:
Customer Mobile Phone:

"Update Debriefing" Frequency:
"Update Debriefing" Time/Location:

Start Date of Vulnerability Assessment:

End Date of Vulnerability Assessment:

Testing will occur at following times:

Will Test be announced to Customer's Target Personnel prior to Test by Customer?

Will Customer Shun IP addresses of attack Systems?

Does the Customer's network have automatic Shunning capabilities that might disrupt access in unforeseen ways (i.e. create a denial-of-service condition), and if so, what steps will be taken to mitigate the risk?:

Would the Shunning of attack systems conclude the test?:

If not, what steps will be taken to continue if systems get shunned and what approval (if any) will be required?:

Will whitelisting be implemented during testing?

List of the relevant IP addresses of Assessment Testing Team's Attack Systems:

4. Annex 3 Definitions

Agreement

Shall mean the Authority & Consent to Test and all applicable Annexes which together shall define the scope of the tests, any rules around the tests and the authority to conduct the tests.

Attack Systems

Shall mean the hardware and software used by Maintel in order to conduct the vulnerability assessment.

Cyber Security

Shall mean technologies, processes and controls designed to protect systems, networks, programs, devices and data from cyber attacks. Effective cybersecurity reduces the risk of cyber attacks and protects against the unauthorised exploitation of systems, networks and technologies.

Penetration Test

Shall mean the level of testing above a vulnerability assessment. During a penetration test exploits are executed against any vulnerabilities discovered. It is possible that this can result in a degradation of hardware/software performance. For this reason, Maintel employees will only perform a vulnerability assessment.

Shun

Shall mean a temporary block at the firewall based strictly on the IP address. Typically shuns are issued for a fixed duration e.g. 24 hours and will expire after that time has passed.

Target Personnel

Shall mean any personnel within the customers business who may have any interaction with the tests performed by Maintel's employees. In the case of a vulnerability assessment, this would usually be IT Staff, Network Operations Centre Staff and/or Security Operations Centre staff.

Tests

Shall mean the manual and automated processes carried out by Maintel Employees in order to discover any vulnerabilities and/or exploits within the scope of the equipment as defined in the Scope Worksheet.

Update Debriefing

Shall mean if the customer requires 'running' updates throughout the vulnerability assessment process the time and frequency of these updates can be specified in the Rules of Engagement document.

Vulnerability Assessment

Shall mean a group of both automatic and manual tests carried out in order to discover any security vulnerabilities and/or potential exploits in the equipment defined in the Scope Worksheet