SERVICE SPECIFIC CONDITIONS FOR CYBER SECURITY SERVICES ("CYBER SECURITY CONDITIONS")

These Cyber Security Conditions apply to the Customer's use of the Cyber Security Services in addition to the Wavenet Master Service Agreement ("MSA")

DEFINITIONS:

Cyber Security Services are delivered by Wavenet's Cyber Security Team ("**Wavenet CyberGuard**").

All definitions from the MSA shall apply to these Cyber Security Conditions, together with the following definitions which shall have the meanings set out below:

"Breach Response" means the structured approach taken to manage, and mitigate a Confirmed Breach;

"Confirmed Breach" means a notification from the Customer confirming that Systems or Data have been compromised due to ransomware, business email compromise or unauthorised System access at an administrative level, or that sensitive or regulated Data has been exposed;

"Consent Form" means an authorisation form or similar document that provides Customer consent to specifics of the Cyber Security Services including testing targets, dates and times;

"**Cyber-attack**" means an attempt by hackers to damage or destroy a computer network or system;

"**Cyber Security Services**" means the Cyber Security Services provided by Wavenet CyberGuard to the Customer under these Cyber Security Conditions and as detailed in the Order;

"**Incident**" means any type of event that may indicate that the Systems or Data have been compromised or that measures put in place to protect them have failed;

"Incident Response" means the structured approach taken to detect, manage, and mitigate security breaches or cyber threats;

"Inclusive Allowance" means a total value of ten thousand pounds (£10,000) plus VAT unless Incident Response Plus is stated on the Order in which case it shall mean a total value of twenty thousand pounds (£20,000) plus VAT, calculated in accordance with Wavenet's standard hourly rates as applicable from time to time;

"CVS Permission Form" means the permission form completed by the Customer to provide the scoping instructions for the CVS Service (as detailed in clause 6) to Wavenet CyberGuard;

"Incident Response Discovery Assessment" means the process whereby Wavenet CyberGuard will collect data regarding the System and existing security tooling for the purpose of supporting incident response engagement;

"**Letter of Engagement**" means an authorisation form or similar document that provides Customer consent to specifics of the Cyber Security Services;

"**24/7 Support Hours**" means 24 hours a day, 7 days a week including English public holidays;

"**Scoping Questionnaire**" means the document detailing the scope and perimeter of the Cyber Security Services to be performed;

"**Security Operations Centre**" means the support facility provided by Wavenet CyberGuard where Systems are monitored and assessed;

"Security Operations Team" means the Wavenet CyberGuard security analysts and management team in the Security Operations Centre; and

"**Security Threat**" means a possible danger that might exploit a vulnerability to breach security of the System and therefore cause possible harm.

1 USE OF THE CYBER SECURITY SERVICES

1.1 Subject to the Customer's payment of the Charges and the terms of this Agreement, Wavenet CyberGuard grants to the Customer a non-exclusive, non-transferable right during the Term to use, and/or allow the End Users to use, the Cyber Security Services and the Software to the extent required for the Customer's internal business operations.

1.2 The Customer shall procure all necessary licences for each End User to use any Customer Software, Third Party Software, and/or Software, which may require the Customer to agree to third party licensing terms, and the Customer warrants that it has and will maintain all necessary licences and consents necessary as part of the Cyber Security Services.

1.3 The Customer shall not, except as may be permitted by Applicable Law or otherwise in accordance with this Agreement:

1.3.1 copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Software in any form or media or by any means; and/or

1.3.2 reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Software.

1.4 The Customer shall not:

1.4.1 modify or alter the Cyber Security Services;

1.4.2 access all or any part of the Cyber Security Services in order to build a product or service which competes with the Cyber Security Services;

1.4.3 use the Cyber Security Services to provide services to third parties; or attempt to obtain, or assist third parties in obtaining, access to the Cyber Security Services, other than as provided under this clause 1; or

1.4.4 sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or make the Cyber Security Services available to any third party except the End Users.

1.5 The Customer agrees that in using the Cyber Security Services that it shall comply with the terms of this clause 1. If the Customer fails to comply with this clause 1 Wavenet CyberGuard shall have the right to:

1.5.1 suspend the Cyber Security Services until such time as it is satisfied that the Customer is able to comply with this clause 1;

1.5.2 terminate the Cyber Security Services forthwith upon written notice to the Customer; and/or

1.5.3 claim any costs, expenses, losses and damages which it may incur as a result of the Customer's failure to comply with this clause 1.

2 WAVENET CYBERGUARD'S OBLIGATIONS

2.1 Wavenet CyberGuard will perform the Cyber Security Services with reasonable skill and care.

2.2 Subject to clauses 2.3 and 2.4 if the Cyber Security Services do not conform to the undertaking in clause 2.1, Wavenet CyberGuard will use reasonable endeavours to correct the defect in accordance with its standard procedures.

2.3 The remedy set out in clause 2.2 constitutes the Customer's sole and exclusive remedy for any breach of the undertaking set out in clause 2.1.

2.4 Notwithstanding the foregoing, Wavenet CyberGuard:

2.4.1 does not warrant that the Customer's use of the Cyber Security Services will be uninterrupted or error-free; nor that it will prevent a Security Threat or Cyber-attack; nor that the Cyber Security Services will meet the Customer's requirements;

2.4.2 is not responsible for any delays, delivery failures, or any other loss or damage resulting from the provision of the Cyber Security Services where such delays or delivery failures are caused by delays or negligence of the Customer and/or any third party outside Wavenet CyberGuard's control, and the Customer acknowledges that the Cyber Security Services may be subject to limitations, delays and other problems inherent in the use of such IT and communications facilities, including Security Threat and Cyber-attack;

2.4.3 shall not be liable to the Customer for any defect in the Cyber Security Services to the extent caused by any defect or failure in the System; and

2.4.4 shall use reasonable endeavours to achieve target dates agreed for delivery but shall be under no liability for any failure to achieve such target dates.

2.5 Subject to the Customer's obligations as set out in the Agreement, Wavenet CyberGuard warrants that it has and will maintain all necessary licences, consents, and permissions necessary for the performance of its obligations under this Agreement.

3 CUSTOMER OBLIGATIONS

3.1 In order for Wavenet CyberGuard to provide the Cyber Security Services the Customer shall provide Wavenet CyberGuard with all necessary co-operation and comply with any obligations in relation to this Agreement and provide access to such information as Wavenet CyberGuard may require, including but not limited to access to the System and any security access information.

3.2 The Customer shall (and ensure its End Users shall):

3.2.1 use the Cyber Security Services in accordance with this Agreement and be responsible for any End User's breach of any term of this Agreement;

3.2.2 comply with any obligations set out in this Agreement;

3.2.3 comply with all Applicable Law and regulations with respect to the Customer's activities under this Agreement;

3.2.4 ensure that the Customer's network and System complies with any relevant specifications provided by Wavenet CyberGuard from time to time; and

3.2.5 be solely responsible for the correction of any defect or failure in the System or network communications.

3.3 The Customer may be required to sign a Consent Form. Wavenet CyberGuard shall not be required to schedule or provide any Cyber Security Services until the Customer has returned such Consent Form duly completed and signed.

3.4 The Customer acknowledges that rescheduling of the Cyber Security Services at short notice would make re-allocation of Wavenet CyberGuard's committed resources to alternative tasks impractical, resulting in Wavenet CyberGuard incurring financial loss. Accordingly, the Customer agrees that, for any notice of rescheduling of Cyber Security Services received by Wavenet CyberGuard prior to the scheduled commencement of the Cyber Security Services, Wavenet may charge a percentage of the Charges for the rescheduled Cyber Security Services ("**Re-Scheduling Charge**") as follows:

3.4.1 less than ten (10) Business Days' notice, payment for 50% of the total project will be charged; and

3.4.2 less than five (5) Business Days' notice, full payment for the project will be charged.

3.5 Upon receipt of any Customer notice provided in accordance with clause 4.4 Wavenet CyberGuard shall re-schedule the Cyber Security Services for a date as soon as reasonably practicable. Where the Customer re-schedules the Cyber Security Services for another date, the Charges for the re-booked Cyber Security Services shall apply in addition to the Re-Scheduling Charges applied in accordance with clause 4.4.

4 LIABILITY AND INDEMNITY

4.1 This clause 4 shall apply in addition to the limitation of liability provisions in the MSA and any limitation of liability specific to a particular service as set out in Schedules 1 and 2.

4.2 Wavenet CyberGuard shall not be liable for any loss or damage to the System which is caused by any existing weakness (or defect) in the System that is discovered or initiated by the provision of the Cyber Security Services from Wavenet CyberGuard.

SCHEDULE 1 - THE CYBER SECURITY SERVICES

The Cyber Security Services to be provided by Wavenet CyberGuard to the Customer may be a combination of the following which will be detailed on the Order.

1 TESTING SERVICES

1.1 The Testing Services will be detailed on the Order and may include vulnerability scanning, penetration testing and wireless testing.

1.2 Upon receipt of a completed Scoping Questionnaire signed by an authorised representative of the Customer, Wavenet CyberGuard will provide the Testing Services on pre-arranged dates to be agreed by the parties.

1.3 The Testing Services will utilise both software applications and manual techniques which may be changed from time to time to comply with Applicable Law and/or software updates

1.4 The Testing Services will aim to identify where the System is at risk of Cyber-attacks using reasonable endeavours.

1.5 Where it is identified as a result of the Testing Services that remediation works are required, the cost of such remediation works is not included within the Agreement.

1.6 The laws of England and Wales apply to the provision of the Testing Services. Some of these laws have particular relevance to technical testing engagements, particularly the Computer Misuse Act, Human Rights Act, and Data Protection Act. Through agreement of Schedule 1 clause 1.7.8 of these Cyber Security Conditions, the Customer agrees to indemnify Wavenet CyberGuard against prosecution for providing the Testing Services.

1.7 The Customer shall:

1.7.1 ensure that the Scoping Questionnaire is completed accurately and by an authorised representative of the Customer;

1.7.2 be responsible for obtaining and maintaining all licences, permissions and consents from third parties prior to the provision of Testing Services;

1.7.3 be wholly responsible for the security of its proprietary and Confidential Information and Data held on the System;

1.7.4 warrant that the System is sufficiently robust to support and facilitate the provision of Testing Services;

1.7.5 maintain up-to-date back-up copies of the configuration for software and hardware and the programs and Data necessary to restore the System to its original state on completion of the provision of the Testing Services and ensure that such back-up copies are kept up to date, in order and available for use at all times;

1.7.6 agree that it will only use the results of the Testing Services for its own internal business purposes and will not disclose the results to any third party without the prior written consent of Wavenet CyberGuard;

1.7.7 indemnify Wavenet CyberGuard, where inaccurate information is provided to Wavenet CyberGuard causing a third-party system to be penetrated; against any claim of illegal activity or infringement, or damages, or loss, whether direct, indirect or consequential resulting from conducting the Testing Services; or where the Testing Services causes damage to the System and a claim is made by a third party;

1.7.8 covenant to Wavenet CyberGuard that it is the sole owner of, or has legal authority to grant access to, the System; and

1.7.9 indemnify Wavenet CyberGuard for any loss, damages, costs, expenses or other claims, howsoever caused through any breach of Schedule 1, clause 1.7.8.

2 DETECT AND RESPOND SERVICES

2.1 The Detect and Respond Services will be detailed on the Order and may include monitoring, vulnerability scanning (see Schedule 1, Testing Services), protection, detection, alerting, investigation, analysis of the System, part of the System, or a combination thereof.

2.2 The Detect and Respond Services will utilise both software applications and manual techniques which may be changed from time to time to comply with Applicable Law and/or software updates.

2.3 Should a Security Threat be detected, the Security Operations Centre will alert the Customer to the Security Threat in accordance with any service levels and escalation process agreed with the Customer on a case-by-case basis.

2.4 It is the Customer's responsibility to act upon notification by the Security Operations Centre of a Security Threat, and to follow the Security Operations Centre's advice which may include contacting the Customer's IT supplier, in-house IT services or purchasing resource in order to respond to the Security Threat.

2.5 Limited remediation services may be provided by the Security Operations Centre as detailed on the Order.

2.6 Any orchestration and automation functionality inherent in the Detect and Respond Services is not designed, intended, or licensed for use in hazardous environments or other applications where a malfunction could cause property damage or personal injury, and Wavenet CyberGuard specifically disclaims any liability in connection with any such use. The Customer assumes all risks in using third-party products or services in connection with the Detect and Respond Services.

3 SECURITY AWARENESS AND TRAINING SERVICES

3.1 The Security Awareness and Training Services will be detailed on the Order and will provide security and awareness training to the End Users in order to help identify potential risks and Security Threats.

3.2 As part of the Security Awareness and Training Services, the Customer will obtain appropriate approval and provide Wavenet CyberGuard with the authority to launch attacks on the System, such as phishing, spear or whaling attacks, which will be randomly generated to target any of the End Users. It is the Customer's responsibility to inform Wavenet CyberGuard in advance with reasonable notice should there be any exceptions made as to End Users who should not be targeted.

3.3 The results from the Security Awareness and Training Services provided are for the Customer's own internal business purposes and neither party will disclose the results to any third party without the prior written consent of the other.

3.4 From time to time, Wavenet CyberGuard will offer training and advice based on current best practice subject to Schedule 2, clause 6.

4 CERTIFICATION SERVICES

4.1 The Certification Services will be detailed on the Order and the Security Operations Team will provide guidance and support to help the Customer to achieve the certification(s).

4.2 It is the Customer's responsibility to ensure that the submissions for the certification(s) are signed by an authorised representative of the Customer; are factually correct and are an accurate representation of the practices implemented within the Customer's business.

4.3 The provision of the Certification Services will not guarantee that the Customer will achieve the certification(s).

5 INCIDENT RESPONSE RETAINER

5.1 The Incident Response Retainer will be detailed on the Order and may include Incident Response such as thorough breach analysis, remediation advice and assistance, guidance with public relations communications, compliance, and recommendations.

5.2 The Customer must agree to and Wavenet CyberGuard will perform an Incident Response Discovery Assessment, which includes collecting relevant technical and network information, and establishing any existing approach to any relevant logging configured on the Customer's network. The cost of this will be included in the Charges or detailed separately in the Order, as applicable. It is the Customer's responsibility to inform Wavenet CyberGuard in advance and in writing with reasonable notice if the Customer intends to make any changes once the Incident Response Discovery Assessment has been completed.

5.3 This Incident Response Retainer is activated upon an email or call to the Security Operations Centre by the Customer.

5.4 The Incident Response Retainer will be detailed on the Order.

5.5 Any use of the Cyber Security Services in excess of the Inclusive Allowance will be charged to the Customer in 60-minute units at Wavenet CyberGuard's discounted hourly rates, either within or outside of Normal Working Hours.

5.6 Service level response times are 2-hour remote response during 24/7 Support Hours.

5.7 In the event that the Customer does not utilise the Incident Response services in any given Contract Year, the Customer shall be entitled to two (2) days of Testing Services or Consultancy Services where Incident Response is stated on the Order, or four (4) days of Testing Services or Consultancy Services where Incident Response Plus is stated on the Order, such Testing Services or Consultancy Services shall be provided by Wavenet CyberGuard for up to 3 months after expiry of the applicable Contract Year and thereafter shall be forfeit.

5.8 The Customer may be required to sign a Letter of Engagement. In such circumstances, Wavenet CyberGuard shall not be obliged to provide any Cyber Security Services until the Customer has returned such Letter of Engagement duly completed and signed. In the event of conflict or ambiguity between the Letter of Engagement and these Service Specific Conditions for Cyber Security Services, such Letter of Engagement will take precedence to the extent of any conflict or ambiguity.

5.9 The following are excluded from the Cyber Security Services:

5.9.1 any payments or facilitation of any payments to any third parties;

5.9.2 the recovery of the Systems or Data;

5.9.3 any software that may be required for any investigation or forensic analysis, which can be made available subject to additional Charges; and/or

5.9.4 any on-site attendance at Customer premises, which can be made available subject to additional Charges.

6 CYBER BREACH RESPONSE RETAINER

6.1 The Cyber Breach Response Retainer is activated upon a call to the Wavenet service desk by the Customer, during which Wavenet will carry out an initial triage to verify a Confirmed Breach.

6.2 During 24/7 Support Hours of a Confirmed Breach, Wavenet shall use reasonable endeavours to make available a member of the Security Operations Team to provide assistance, recommendations, and guidance for initial containment.

6.3 As necessary and on the next Business Day following a Confirmed Breach, Wavenet will form a team to provide Breach Response which may include forensic analysis, log collection, remediation advice and assistance, third party collaboration, and/or regulatory reporting advice and guidance.

6.4 A minimum amount of five thousand pounds (£5,000) shall be deducted from the Inclusive Allowance for every Confirmed Breach reported by the Customer.

6.5 Any use of the Cyber Security Services in excess of the Inclusive Allowance will be charged to the Customer in 60-minute units at Wavenet's standard hourly rates, either within or outside of Normal Working Hours as applicable.

6.6 The Customer may be required to sign a Letter of Engagement. In such circumstances, Wavenet CyberGuard shall not be obliged to provide any Cyber Security Services until the Customer has returned such Letter of Engagement duly completed and signed. In the event of conflict or

ambiguity between the Letter of Engagement and these Service Specific Conditions for Cyber Security Services, such Letter of Engagement will take precedence to the extent of any conflict or ambiguity.

6.7 The following are excluded from the Cyber Security Services:

6.7.1 any payments or facilitation of any payments to any third parties;

6.7.2 the recovery of the Systems or Data;

6.7.3 any software that may be required for any investigation or forensic analysis;

6.7.4 any on-site attendance at Customer premises, which can be made available subject to additional Charges;

6.7.5 any legal or public relations advice; and/or

6.7.6 Services in relation to any Confiirmed Breach relating to the Customer's operations located outside of the United Kingdom.

7 CONTINUOUS VULNERABILITY SCANNING ("CVS SERVICE")

7.1 The CVS Service will be detailed on the Order and may include vulnerability scanning, reporting and compliance support, and vulnerability prioritisation advice. The CVS Service is available during Normal Working Hours only.

7.2 Upon completion of the CVS Permission Form, signed by the Customer's authorised representative, Wavenet will provide the CVS Service on pre-arranged dates to be agreed between both parties.

7.3 Should a vulnerability be detected, the report will alert the Customer to the Security Threat and it is the Customer's responsibility to act upon the notification of a Security Threat and to follow the advice, which may include contacting the Customer's IT supplier, in-house IT services, or purchasing resource in order to respond to the Security Threat.

7.4 The Order will specify the scanning solution used for the CVS Service.

7.5 Where the Qualys Cloud-Based Vulnerability Platform ("**Qualys Application**") is used the Customer accepts that:

7.5.1 the Qualys Application may be changed from time to time to comply with Applicable Law and/or software updates; and

7.5.2 Qualys owns the Qualys Application, and the Customer will not receive any licence or right to use the Qualys Application, which is provided "as is". Qualys disclaims all express or implied warranties regarding the Qualys Application and shall not have any liability to the Customer for either direct, indirect or consequential damages. The Customer hereby consents to the Qualys Application processing and storing the Customer's personal data outside the EEA.

SCHEDULE 2 – GENERAL

1. The Security Operations Centre will operate via telephone or remotely during 24/7 Support Hours.
2. Where applicable, on-site visits will take place during Normal Working Hours, unless agreed otherwise in advance.
3. The Customer agrees to the Security Operations Centre being able to access its System in order to perform the Cyber Security Services.
4. As part of the provision of the Cyber Security Services, the Customer may be required to agree to third party licensing terms.
5. The Customer's usage of the Cyber Security Services should be reasonable and fair. Should the Customer's usage be deemed excessive, including the storage of any data as required for the provision of the Cyber Security Services, as determined by Wavenet in a commercially reasonable manner, Wavenet may require the Customer to purchase additional Cyber Security Services.
6. The Customer acknowledges that the provision of these Cyber Security Services, including the use of third-party services, does not provide a guarantee against Cyber-attacks or Security Threats or that the System is or will be free from every form of attack, flaw, or security weakness.