Interfuture Systems Limited

Security Services Schedule

1. Definitions applicable to this Schedule:

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

   "**Cyber-attack**" means an attempt by hackers to damage or destroy a computer network or system or to extort money through data encryption and ransomware.

   "**Incident**" means an Incident is any type of event that may indicate that the Customer's Systems or Data have been compromised or that measures put in place to protect them have failed.

   "**Rules of Engagement**", means the rules of engagement provided by Interfuture to the Customer from time to time detailing the services to be carried out by Interfuture.

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

   "**Third Party Services**" means any software or services provided to you by Interfuture on behalf of a third-party provider.

2. Interfuture's Obligations

   2.1 Interfuture will perform the Services with reasonable skill and care, except to the extent that the Customer has failed to comply with its obligations in this Contract and the Rules of Engagement, or where the Customers use of the Services is contrary to Interfuture's instructions, or where the Services have been modified or altered by anyone other than Interfuture or its authorised contractors or agents;

   2.2 Notwithstanding the foregoing, Interfuture:

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

   2.2.2 is not responsible for any delays, delivery failures, or any other loss or damage resulting from the provision of Services, and the Customer acknowledges that the 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; and

2.2.3 shall not be liable to the Customer for any defect in the Services to the extent caused by any defect or failure in the Customer's System

2.3 Subject to the Customer's obligations as set out in this Contract and the Rules of Engagement, Interfuture warrants that it has and will maintain all necessary licences, consents, and permissions necessary for the performance of its obligations under this Contract and the Rules of Engagement.

3. Customer Obligations

3.1 In order for Interfuture to provide the Services the Customer shall be required to sign and agree to the Rules of Engagement and shall provide Interfuture with all necessary co-operation and comply with any obligations in relation to this Contract and the Rules of Engagement, and access to such information as Interfuture may require, including but not limited to access to the Customer's System and any security access information.

3.2 The Customer hereby acknowledges that Interfuture is under no obligation to provide any services until the Rules of Engagement have been signed by the Customer.

3.3 The Customer shall and shall ensure its end users, including but not limited to its employees, freelancers, contractors and workers (Authorised Users):

3.3.1 agree and adhere at all times to the Rules of Engagement provided by Interfuture from time to time to the Customer;

3.3.2 use the Services in accordance with this Contract and the Rules of Engagement provided form time to time and be responsible for any Authorised User's breach of any term of this Contract and the Rules of Engagement;

3.3.3 comply with any obligations set out in this Contract and the Rules of Engagement;

3.3.4 comply with all Applicable Laws and regulations with respect to the Customer's activities under this Contract and the Rules of Engagement;

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

3.3.6 be solely responsible for the correction of any defect or failure in the Customer's System or network communications

3.4 The Customer hereby warrants and agrees that it shall ensure all Authorised Users who have access to any system, software or other Services provided at any point by Interfuture are fully aware of the Services to be provided in accordance with this Schedule and the Rules of Engagement.

3.5 In accordance with this Schedule and the Rules of Engagement, the Customer understands and agrees that Interfuture shall harvest logs and data from the system, software and machines used by the Customer, its Authorised Users and any other third party, and the Customer hereby confirms and warrants that it has sufficiently notified all individuals who have access to any system, software, hardware or other Services that such logs will be collected. The Customer further warrants that it has obtained all necessary sign off and approvals from its Authorised Users and any other third party prior to Interfuture carrying out the Services.

4. Liability And Indemnity

4.1 This clause applies in addition to the limitation of liability provision in the Contract and any limitation of liability specific to a particular service provided.

4.2 The Customer assumes sole responsibility for results obtained from the use of the Services and any Software, and for conclusions drawn from such use. Interfuture shall have no liability to the Customer, its Authorised Users or any third parties for any damage caused by any action taken by Interfuture as well as any errors or omissions in any information or instructions provided to Interfuture by the Customer in connection with the Services and/or any Software, or any actions taken by Interfuture at the Customer's direction.

4.3 The Customer understands that the services to be provided in accordance with this Schedule and the Rules of Engagement are highly intrusive and the Customer hereby fully indemnifies Interfuture against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other professional costs and expenses) suffered or incurred by Interfuture arising out of or in connection with any claim made by an Authorised User or any other third party arising out of or in connection with the provision of the Services, to the extent that such claim arises out of the breach, negligent performance or failure or delay in performance of this Contract, including any obligations under this Schedule and the Rules of Engagement, by the Customer.

4.4 The Customer understands and accepts that such Services under this Schedule may cause downtime to other Services and Interfuture shall not be liable or responsible for any such downtime and the provisions of any other support or maintenance Services provided under this Contract shall not be applicable.

5. The Services

5.1 The Services to be provided by Interfuture to the Customer may be a combination of the following which will be detailed on the Order Form.

5.2 Testing Services

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

5.2.2 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 updates

5.2.3 The Testing Services will aim to identify where the Customer's System is at risk of Cyber-attacks using reasonable endeavours

5.2.4 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

5.2.5 The Customer shall:

5.2.5.1 Be responsible for obtaining and maintaining all licences, permissions and consents from third parties prior to the provision of Testing Services being provided

5.2.5.2 Be wholly responsible for the security of its propriety and Confidential Information and Data held on the System

5.2.5.3 Warrant that the System is sufficiently robust to support and facilitate the provision of Testing Services

5.2.5.4 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 and in order and available for use at all times

5.2.5.5 Agree that it will only use the results of the Services provided for its own internal business purposes and will not disclose the results to any third party without the prior written consent of Interfuture

5.2.5.6 Indemnify Interfuture, where inaccurate information is provided to Interfuture causing a third-party System to be penetrated, against any claim of illegal activity or infringement, or damages, or loss, whether proximate or consequential resulting from conducting the Testing Services, or where the Testing Services causes damage to the Customer's System and a claim is made by a third party

5.3 Detect And Respond Services

5.3.1 The Detect and Respond Services will be detailed on the Order Form and may include monitoring, vulnerability scanning (see clause 5.2, Testing Services), protection, detection, alert, investigation, analysis of the Customer's System or part of the Customer's System, or a combination thereof

5.3.2 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 updates

5.3.3 Should a Security Threat be detected, Interfuture will alert the Customer to the Security Threat within its operating hours and in accordance with its service levels. Interfuture shall determine the best cause of action following a Security Threat being detected and shall notify the Customer of this. The Customer warrants and acknowledges that this may involving shutting down access to the Services until the incident has been resolved.

5.3.4 The Customer must notify Interfuture of any risks that may cause a Security Threat the Services such as a Customer user travelling and accessing the system internationally.

5.3.5 Where necessary, it is the Customer's responsibility to act upon the notification by Interfuture of a Security Threat, and to follow Interfuture's advice which may include contacting the Customer's IT supplier, in-house IT services or purchasing labour in order to respond to the Security Threat.

5.4 Security Training Services

5.4.1 The Security Training Services will be detailed on the Order Form. Following a penetration test Interfuture will provide security training to the Customer's staff in order to help identify potential risks and Security Threats

5.4.2 As part of the Services to be provided, the Customer will obtain appropriate approval and provide Interfuture with the authority to

launch attacks on the Customer's System, such as phishing, spear or whaling attacks, which will be randomly generated to target any of the Customer's Authorised Users. It is the Customer's responsibility to inform Interfuture in advance with reasonable notice should there be any exceptions made as to Authorised Users who should not be targeted

5.4.3 The results from the 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

5.5 Certification Services

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

5.5.2 It is the Customer's responsibility to ensure that the submission 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

5.5.3 The provision of these Services will not guarantee that the Customer you will achieve the certification(s)

5.6 Incident Response

5.6.1 The Incident Response will include Services such as thorough breach analysis, remediation advice and assistance, guidance with PR and compliance, and recommendations

5.6.2 The Customer must agree to and Interfuture will perform an annual Pre-Incident Assessment, which includes collecting relevant technical and network information, making recommendations for the Customer's current incident response plan and ensuring that relevant logging is configured on the Customer's network. The cost of this will be detailed in the Order Form. It is the Customer's responsibility to inform Interfuture in advance and in writing with reasonable notice if the Customer intends to make any changes once the annual Pre-Incident Assessment has been completed.

5.6.3 The Incident Response will comprise of service level response times being 2-hour remote response, which operates 24/7, and next day on-site response (where an Incident is reported before 2pm).

5.7 Vulnerability Management Service

5.7.1 The Vulnerability Management Service will be detailed on the Order Form and may include vulnerability scanning, reporting and compliance support (the Standard Level) and vulnerability prioritisation advice and Interfuture support (the Enhanced Level). This Service is available during our Normal Support Hours only

5.7.2 Interfuture will provide the agreed Vulnerability Management Service on pre-arranged dates to be agreed between both parties

5.7.3 Should a vulnerability be detected, the report will alert the Customer to the Security Threat and it is your responsibility to act upon the notification by Interfuture of a Security Threat and to follow the advice..