Managed Services Schedule

Version 1.0

1. APPLICATION AND INTERPRETATION

1.1 This Managed Services Schedule forms part of Penny Apples' General Terms and Conditions and applies in addition to the General Terms for any Contract for the provision of Managed Services provided by the Supplier to the Customer. Where not explicitly defined in this schedule all capitalised terms herein shall be interpreted in accordance with the definitions in the General Terms. Where the General Terms conflict with this Managed Services Schedule the latter shall take precedence.

1.2 Not used.

1.3 The definitions and rules of interpretation in this paragraph apply to terms used in this Schedule. All other capitalised terms are as described and interpreted in accordance with Penny Apples' General Terms ('General Terms'). Acceptance Date: has the meaning given in paragraph 2.7. Additional Services: Services which are not part of the Managed Service, Set-up Service or Maintenance Services which the Supplier offers to the Customer at an additional fee. Assets: any Customer-site Equipment, Software or Intellectual Property Rights used by the Supplier exclusively for the delivery of the Managed Services to the Customer. Assumed Contracts means the contracts specified in the Managed Services Description currently in the name of the Customer which the Customer shall assign or otherwise arrange for the Supplier to become a party to for use in the Managed Services. Change Control Procedure: the procedures set out in paragraph 6. Customer Account Team: the individuals appointed by the Customer from time to time who shall serve as the Supplier's primary contacts for the Supplier's activities under this schedule. Customer Data: any information that is provided by or on behalf of the Customer to the Supplier as part of the Customer's use of the Services, including any information derived from such information. Customer Policies: those policies notified to and accepted by the Supplier. Customer Site: any premises occupied by the Customer at which it receives the Managed Services. Customer's Project Manager: the member of the Customer Account Team appointed by the Customer from time to time, the first of which will be named in the Managed Services Description.

Error: has the meaning given in Paragraph 2.5. Extended Term: has the meaning given in Paragraph 14.1. Managed Service Fees: the price payable to the Supplier for all fees payable under this Managed Services schedule including the Set -up Fees, the Monthly Fees and the Maintenance Fees , as further described in paragraph 9 and stated on the Acknowledgement and. Hardware: all physical telecommunications, networking and computer equipment (including switches, routers, cables, servers, racks, cabinets and peripheral accessories) provided and used by the Supplier to deliver the Managed Services to the Customer. Incident: any known or latent Vulnerability, Virus or known security incident which: a. may affect the Assets; b. may affect the Supplier's network and information systems such that it could potentially affect the Customer or the Assets; or c. is reported to the Supplier by the Customer. Initial Term: the period from the Commencement Date until the third anniversary of such date; Known Vulnerability: any Vulnerability that has either: a. been assigned a Common Vulnerabilities and Exposures (CVE) number; b. been disclosed on the National Vulnerability Database available at the website operated by the US National Institute of Standards and Technology (NIST) from to time to time; or c. been disclosed on the internet, or any public database, such that it would be revealed by reasonable searches conducted in accordance with Good Industry Practice. Latent Vulnerability: any instances of typical classes of Vulnerability. For example, buffer overflows, cross -site scripting (XSS) and Structure Query Language (SQL) injection.

Maintenance Services: any error corrections, updates and upgrades that the Supplier may provide or perform with respect to the Managed Services, as well as any other support or training services to be provided to the Customer under this schedule, all as described in Managed Services Description. Maintenance Events: has the meaning given in Managed Services Description. Managed Services Description: means the managed services description in the sub - schedule below setting out all the technical and procedural information required for the Managed Services to be delivered in accordance with this Schedule. Mitigate: the taking of such reasonable steps that would be taken by a prudent supplier in accordance with industry practice to mitigate against the Incident in question, which may include (in the case of a Vulnerability) coding changes, but could also include Managed Services Description changes (for example, removal of affected protocols or functionality in their entirety), provided these are approved by the Customer in writing in advance, and the terms Mitigated and Mitigation shall be construed accordingly. Priority 1, 2, 3 and 4 incidents: have the meanings given in the Service Level Schedule within the Sub Schedule. Project Plan: the plan to be developed in the planning stage of the Set-up Services. Quarterly Meetings: has the meaning given in Paragraph 11.1. Regulatory Requirement: has the meaning given in Paragraph 14.11. Replacement Supplier: any entity with which the Customer contracts (or proposes to contract) to provide services similar to all or any of the Managed Services and Maintenance upon the expiry or termination of all or any part of this schedule for any reason. Review Meeting: has the meaning given in Paragraph 11.3. Service Credit means the percentage of the monthly cost for Managed Services that is awarded to the Customer for a validated claim associated with that portion of the Support Services related to breach of the SLA during that month. Service Level Arrangements: the service level arrangements set out in the Managed Services Description. Services: the Set -up

Services, the Managed Services, the Maintenance and the Transition Services. Set-up Services: the due diligence, configuration and related work referred to in the Managed Services Description, to be performed by the Supplier to set up the Managed Services. Software: any software used by the Supplier (or any of its sub -contractors) to provide the Managed Services to the Customer whether owned by a third party (Third Party Software:), by the Customer (Customer Software :) or by the Supplier (Supplier Software:). Supplier Account Team: the individuals appointed by the Supplier from time to time who shall serve as the Customer's primary contacts for the Customer's activities under this schedule. Supplier's Project Manager: the member of the Supplier's Account Team appointed in accordance with Paragraph 2.2. The Supplier's Project Manager at the Commencement Date is named in the Managed Services Description. Supplier Software: has the meaning given to that term in the definition of Software. Supplier's System: the information and communications technology system to be used by the Supplier (or any of its sub -contractors) in performing the Services, including the Hardware, the Software, the Customer -site Equipment and communications links between the Hardware and the Customer-site Equipment and the Customer's Operating

Environment. Transferring Contracts: the third -party contracts (including licences to Third -Party Software) that the Supplier reasonably considers necessary to enable the transition of the Managed Services to the Customer or any Replacement Supplier on expiry or termination of all or any part of this schedule for any reason. Transition Services: the services to be provided by the Supplier on termination of this schedule which shall mean the provision of systems documentation which shall be provided at termination and any Additional Services agreed between the parties for the payment of Additional Fees.. Virus: includes any malicious code, Trojan, worm and virus, lock, authorisation key or similar device that impairs or could impair the operation of the Software or the Managed Services. Vulnerability: a weakness in the computational logic (for example, code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability, and the term Vulnerabilities shall be construed accordingly. Work Product: all deliverables and all other reports, documents, materials, techniques, ideas, concepts, trademarks, know -how, algorithms, software, computer code, routines or sub-routines, service descriptions, plans, notes, drawings, designs, pictures, images, text, audio visual works, inventions, data, information and other items, expressions, works of authorship or work product of any kind that are authored, produced, created, conceived, collected, developed, discovered or made by the Supplier (or any of its sub-contractors) in connection with the Services or which relate in any manner to the Services or which result from any work performed by the Supplier (or any of its sub -contractors) for the Customer, including any and all Intellectual Property Rights therein.

1.4 Any Goods agreed to be supplied by the Supplier and necessary for the Managed Services, including but not limited to Hardware, Software, documentation and licences thereto shall be provided by the Supplier to the Customer in accordance with the General Terms before Set-up Services are initiated.

1.5 Not used.

1.6 Where the Customer is supplying the Customer Site Equipment required for the Managed Service the Customer shall follow the Supplier's instructions for making the Customer Site Equipment ready for the integration of the Managed Services with the Customer's system.

1.7 The Customer shall on the Commencement Date ensure that the benefit of any Assumed Contracts are assigned, novated or transferred to the Supplier as soon as practicable and in any event before the initiation of the Start-up Services. If any consent of any third party is required to the assignment, novation or transfer of an Assumed Contract and has not been obtained at, or prior to, the Commencement Date, the Customer and the Supplier shall each use all reasonable endeavours to obtain that consent as soon as possible after the Commencement Date. Unless or until any Assumed Contract is assigned, novated or transferred, or any necessary consent is obtained, the parties shall work together, in good faith, to agree an alternative solution which may include the Supplier finding an alternative source of supply and/or the Customer holding the benefit of the releva nt Assumed Contract as agent for the Supplier.

Inherited Technology: means any software, hardware, system, service, configuration or component installed, supplied, configured, operated, accessed or used before the Commencement Date by the Customer, a previous managed service provider, an incumbent supplier or any other third party. It includes residual, dormant, obsolete or undocumented remote monitoring and management tools, support agents, remote-access software, antivirus, endpoint-detection, backup, monitoring and security software, accounts, credentials, certificates, authentication tokens, encryption keys, scripts, scheduled tasks, automation, policies, integrations, connectors, application programming interfaces, firewall rules, network configurations, virtual machines, cloud resources and other components remaining from a previous support arrangement.

Inherited Vulnerability: means any vulnerability, malware, virus, unauthorised access mechanism, insecure configuration, unsupported component, compromised credential or other security weakness that existed within, arose from, or was introduced through Inherited Technology before the Commencement Date.

Cyber and Data Event: means any actual or alleged cyberattack, security incident, malware, ransomware, virus, vulnerability, loss, destruction, alteration, corruption or unavailability of Customer Data, unauthorised access to or disclosure of Customer Data, personal-data breach, failure of any backup, disaster-recovery, remote-monitoring, management, support, security or

communications tool, Inherited Technology or Inherited Vulnerability, or any failure to detect, prevent, mitigate, patch, remediate, report or respond to any such matter.

2. SET-UP SERVICES

2.1 The Supplier Account Team shall initially consist of the personnel stated by the Supplier at the start of the contract . The Supplier shall use reasonable endeavours to ensure continuity of its personnel assigned to this schedule.

2.2 The Supplier shall appoint the Supplier's Project Manager, who shall have the authority to contractually bind the Supplier on all matters relating to this schedule. The Supplier shall use reasonable endeavours to ensure continuity of the Supplier's Project Manager but has the right to replace him/her from time to time where reasonably necessary in the interests of the Supplier's business.

2.3 The Supplier shall prior to providing any of the Set -up Services survey the Customer Site and make any necessary adjustments to the Managed Services Description to reflect the requirements of the building and Customer Operating Environment. Where the change in the Managed Services Description resulting from such survey adjustment increases the price of the Managed Services the Supplier shall notify the Customer and providing the increase is less than 10% more than the initial price the Customer shall pay such higher figure. Where the amount of increase exceeds 10% the Customer and the Supplier shall use the change control procedure to agree the price and where agreement proves impossible this Contract shall be terminated at the option of either party without further liability to the other in respect of the failure to provide the Managed Services in accordance with the Contract.

2.4 The Supplier shall perform the Set -up Services in accordance with the Managed Services Description. The Supplier shall use reasonable endeavours to meet any agreed performance dates, but any such dates shall be estimates only, and time shall not be of the essence in this schedule.

2.5 When the Supplier considers that following installation the Managed Services are ready for activation it shall so notify the Customer. Within five Business Days of such notification the Customer shall review the operation of the Managed Services to confirm that they function in material conformance with the Managed Services Description. If the Managed Services fail in any material respect to conform with the Managed Services Description, the Customer shall give the Supplier a detailed description of any such non- conformance (Error) in writing, within the five Business Day review period.

2.6 The Supplier shall use reasonable endeavours to correct any Error within a reasonable time and, on completion, re -submit the Managed Services to the Customer. The provisions of Paragraph 2.4 and this Paragraph 2.5 shall then apply again, up to three additional times. If the Supplier is unable to correct the Error after three attempts, either party may terminate this schedule with immediate effect by giving written notice to the other party, without further liability to the other in respect of the Error or failure to provide the Managed Services in accordance with this schedule.

2.7 If the Managed Services are found to conform with the Managed Services Description or if the Customer does not provide any written comments within the five Business Day review period described in Paragraph 2.4 , the Managed Services shall be deemed accepted as from the date of the notification or expiry of the five Business Day review period (in each case the Acceptance Date).

2.8 Where the Set -Up Services consist purely of a due diligence exercise on an existing system as described further in the Managed Services Description then once the due diligence exercise is complete and the Supplier is satisfied with the Customer Operating Environment for the provision of the Managed Services the Supplier shall communicate this to the Customer and the date of this communication shall be the Acceptance Date.

2.9 Where following the due diligence exercise the Supplier concludes, at its sole but reasonable discretion, that the Customer Operating Environment is unsatisfactory the Customer may choose to either:

2.9.1 upgrade the Customer Operating Environment:

2.9.1.2 itself and complete further due diligence at an additional cost to be agreed with the Supplier; or

2.9.1.3 request the Supplier to adjust the Managed Services Description at an additional cost to include the necessary upgrade (in which case the usual installation testing procedures shall apply); or

2.9.2 choose to terminate the Contract providing a payment is made to reimburse the Supplier for the reasonable costs of the due diligence exercise.

2.10 INHERITED TECHNOLOGY - TRANSITION AND DISCOVERY

2.10.1 During the transition and onboarding period stated in the Managed Services Description, the Supplier shall use reasonable care and skill to undertake the discovery and assessment activities expressly included within the agreed onboarding

scope.

2.10.2 The Customer acknowledges that Inherited Technology may be concealed, dormant, undocumented, inaccessible or otherwise incapable of being identified through reasonable discovery activities. The Supplier does not warrant that onboarding, audit, monitoring or discovery activities will identify every item of Inherited Technology or every Inherited Vulnerability.

2.10.3 The Customer shall provide complete and accurate information concerning its systems, suppliers, former service providers and support arrangements; provide all reasonably required credentials, access rights, records and asset information; procure reasonable cooperation from previous service providers and other suppliers; notify the Supplier of known or suspected residual tools, remote-access facilities, compromised credentials or security concerns; and authorise the Supplier to disable, isolate or remove Inherited Technology where reasonably necessary to protect the Customer Operating Environment.

2.10.4 Where the Supplier identifies Inherited Technology or an Inherited Vulnerability, it shall notify the Customer within a reasonable period and recommend appropriate mitigation, isolation, removal, replacement or remediation. Work outside the agreed onboarding scope or Managed Services Description shall be an Additional Service subject to additional Charges.

2.10.5 The Supplier may immediately suspend, isolate or disable Inherited Technology where it reasonably considers that continued operation creates a material security risk and shall notify the Customer as soon as reasonably practicable.

2.10.6 Inherited Technology shall not become part of the Supplier's managed environment merely because it is discovered, monitored or temporarily accessed by the Supplier. It shall become managed technology only when expressly accepted into scope in writing or included in an agreed Managed Services Description.

3. MANAGED SERVICE PROVISION

3.1 The Supplier shall provide the Managed Services (including the Maintenance Services) from the Acceptance Date until expiry or termination of this schedule for any reason.

3.2 The Service Level Arrangements shall apply with effect from the start of the first complete month occurring at least 30 days after the Acceptance Date.

3.3 The Customer shall comply, and ensure all Authorised Users comply, with all third party and Supplier licences and shall not store, distribute or transmit through the Managed Services any material that:

3.3.1 is unlawful, fraudulent, harmful, threatening, defamatory, obscene, harassing or racially or ethnically offensive;

3.3.2 facilitates illegal activity or depicts sexually explicit images;

3.3.3 promotes unlawful violence, discrimination based on race, gender, age, disability, sexual orientation, religion, belief or gender reassignment, or any other illegal activity; and/or

3.3.4 in any other way breaches the licences in relation to any of the Goods used in the provision of the Managed Services.

3.4 The Customer shall not use the Service:

3.4.1 in a way that does not comply with the terms of any legislation or any licence applicable to the Customer or in any way that is unlawful or fraudulent or has any unlawful or fraudulent purpose or effect;

3.4.2 to send, knowingly receive, upload, download, use or re-use any material which is abusive, indecent, defamatory, obscene or menacing, or in breach of any copyright, confidence, privacy or any other similar rights.

3.4.3 to send or procure the sending of any unsolicited advertising or promotional material other than in the case of the Customer to its own Customers.

3.4.4 in a way that does not comply with any reasonable operating instructions the Supplier has given.

3.4.5 in connection with the carrying out of a fraud or criminal offence against Penny Apples, or any public telecommunications operator;

3.5 The Supplier reserves the right to:

3.5.1 modify the Supplier’s System, its network, system configurations or routing configuration; or

3.5.2 modify or replace any Hardware or Software in its network or in equipment used to deliver any Service over its network, provided that this has no adverse effect on the Supplier’s obligations under this schedule and its provision of the Services or the Service Level Arrangements. If such changes will have an adverse effect, the Supplier shall notify the Customer and the parties shall follow the Change Control Procedure.

3.5.3 At its option suspend and/or terminate the Managed Services should the Supplier reasonably believe the provisions or paragraph 3.3, 3.4 or 3.5 have been breached.

3.6 The Supplier shall comply with the Customer Policies at all times when providing the Services at the Customer's Sites.

3.7 As part of the Managed Service the Supplier offers Maintenance Services by telephone, remote access using TeamViewer and by on Customer Site assistance subject to Service Levels based on priority requirements and the terms of the Service Level Schedule within the Managed Services Description .

4. SUPPLIER'S OBLIGATIONS

4.1 The Supplier undertakes that the Managed Services will be provided substantially in accordance with the Managed Services Description and the warranty requirements (and subject to the limitations) of the General Terms. For the avoidance of doubt the exclusions stated in the SLA and the Assumptions apply to the undertaking under this

Paragraph 4.1 and the Supplier shall not be under any obligation to carry out services in in respect of the exclusions specified or where the Assumptions prove incorrect.

4.2 The undertaking in Paragraph 4.1 shall not apply to the extent of any non-conformance that is caused by use of the Managed Services contrary to the Supplier's instructions.

4.3 If the Services do not conform with the undertaking in Paragraph 4.1, the Supplier shall, at its expense, use all reasonable commercial endeavours to correct any such non - conformance promptly, or provide the Customer with an alternative means of accomplishing the desired performance. Such correction or substitution constitutes the Customer's sole and exclusive remedy for any breach of the undertaking in Paragraph 4.1.

4.4 Notwithstanding the foregoing, the Supplier does not warrant that the Customer's use of the Managed Services shall be uninterrupted or error-free.

4.5 Arrangements for planned maintenance events and provisions relating to emergency maintenance events and the resulting downtime of the Managed Services shall be arranged and managed in accordance with the provisions for maintenance expressed in Sub- Schedule 3.

4.6 This schedule shall not prevent the Supplier from entering into similar schedules with third parties, or from independently developing, using, selling or licensing materials, products or services that are similar to those provided under this schedule.

5. CUSTOMER'S OBLIGATIONS

The Customer shall:

5.1 provide the Supplier with:

5.1.1 all necessary co-operation in relation to the Services; and

5.1.2 all necessary access to such information as may be reasonably required by the Supplier, in order to provide the Services, including Customer Data, security access information, and (subject to providing any confidentiality undertakings reasonably required by the Customer) software interfaces to the Customer's other business applications;

5.2 provide such personnel assistance, including the Customer Account Team and other Customer personnel, as may be reasonably requested by the Supplier from time to time. The Customer Account Team shall initially consist of the personnel listed in the Managed Services Description.

5.3 appoint the Customer's Project Manager, who shall have the authority to contractually bind the Customer on all matters relating to this schedule. The Customer shall use reasonable endeavours to ensure continuity of the Customer's Project

Manager, but has the right to replace them from time to time where reasonably necessary in the interests of the Customer's business;

5.4 comply with all applicable laws and regulations with respect to its activities under this schedule;

5.5 carry out all other Customer responsibilities set out in this schedule or in the Managed Services Description in a timely and efficient manner. In the event of any delays in the Customer's compliance with their obligations under this Schedule the Supplier may adjust any timetable or delivery schedule set out in this schedule as reasonably necessary.

5.6 The Customer Operating Environment connected to or used with the Managed Services must be connected and used in accordance with any reasonable instructions, safety and security procedures applicable to the use of the Customer Operating Environment. Where t he Customer Operating Environment is attached (directly or indirectly) to the Managed Services it must be

technically compatible with the Managed Services and approved for the purpose under any relevant legislation or telecommunications industry standards.

5.7 The Customer shall not:

5.7.1 allow the Managed Services to be repaired or maintained except by an authorised representative of the Supplier;

5.7.2 damage the Customer -site Equipment and not add or modify or in any way interfere with the performance of the Customer-site Equipment;

5.7.3 provide the Managed Services directly or indirectly to third parties (with the exception that hotel guests may use the Managed Services designed for hotel guest use subject to the guest accepting the limitations on use stated in paragraph 3.3 or 3.4 above);

5.7.4 not remove any identification mark affixed to the Customer -site Equipment showing that it is the property of the Supplier or other third -party supplier of such equipment.

6. CHANGE CONTROL

6.1 If either party wishes to change the scope of the Managed Services (including Customer requests for additional services), it shall submit details of the requested change to the other in writing.

6.2 If either party requests a change to the scope or execution of the Services, the Supplier shall, within a reasonable time, provide a written estimate to the Customer of:

6.2.1 the likely time required to implement the change;

6.2.2 any variations to the Managed Services Fees arising from the change;

6.2.3 the likely effect of the change on the Project Plan; and

6.2.4 any other impact of the change on the terms of this schedule.

6.3 If the Supplier requests a change to the scope of the Services, the Customer shall not unreasonably withhold or delay consent to it. If the Customer requests a change pursuant to Paragraph 10, or a change is proposed pursuant to Paragraph 11, the Supplier shall not unreasonably withhold or delay consent to it.

6.4 If either party wishes the other party to proceed with the relevant change referred to in Paragraph 6.3, the Supplier has no obligation to do so unless and until the parties have agreed in writing the necessary variations to its charges, the Project Plan and any other relevant terms of this schedule to take account of the change.

6.5 For the avoidance of doubt any change of regulation or law which affects this contract shall be viewed as a change request at the request of the Supplier. The Supplier will comply with Paragraph 14.11 with respect to the regulatory/legal change and supply the Customer with the variation required and the Customer may accept the change or terminate this schedule on notice and pay any termination charges in accordance with paragraph 14.6.1 if still within the Initial Period.

7. SECURITY

7.1 The Supplier shall ensure that the Managed Services are provided with appropriate safety and security systems, policies and procedures detailing how to prevent unauthorised access or damage to, any and all Services, the Supplier's System and related networ ks or resources and the Customer Data, in accordance with industry practice. The Customer agrees to comply with all safety and security instructions given by the Supplier during the course of the Managed Services and to implement all reasonable policies and procedures notified by the Supplier for the necessary safety and security of the Customer Operating Environment.

7.2 The Supplier shall ensure that the Supplier's System is designed, maintained and notifications relating to necessary upgrades are provided in a timely fashion (subject to additional costs) so as to Mitigate against Incidents. The parties agree that if Inc idents are detected or discovered, each of them shall co-operate with the other to Mitigate the Incident and, particularly if the Incident causes or threatens the loss of operational efficiency, loss or corruption of Customer Data, or the reduced manag ement of risks posed to the security of the Assets, the Supplier's System, or the Customer's Operating Environment, the parties shall assist each other to Mitigate any losses and restore the Services to their original operating and security efficiency. The costs of complying with this Paragraph 7.2 shall be apportioned between the parties on a pro rata basis according to fault.

7.3 The Customer shall promptly inform the Supplier if it suspects or uncovers any Incident and, subject to the cost allocations in Paragraph 7.2 , shall use all commercially reasonable endeavours to promptly Mitigate such Incident.

7.4 Third party usage and hacking: The Customer shall remain responsible for the use of the Managed Services under its control, including any use by third parties (whether fraudulent or invited by the Customer). The Customer accepts that the Managed

Services have the potential to be hacked and will use best endeavours to protect the Managed Services from third party hacking including using passwords which are regularly updated, secure locations and training for personnel using the system. Any recharged usage charges incurred through PBX hacking or hacking of any other kind shall be borne by the Customer and not the Supplier unless due to the material negligence of the Supplier. The Supplier shall use reasonable endeavours to alert the Customer to any hacking as soon as practicable but is not liable for any damage caused prior to and within a reasonable time after becoming aware of the hacking. The Customer agrees to indemnify the Supplier in respect of any costs incurred by the Supplier in making the Managed Services safe again unless due to the material negligence of the Supplier.

7.5 The Supplier shall:

7.5.1 notify the Customer immediately it becomes aware of any Incident and respond without delay to all queries and requests for information from the Customer about any Incident, whether discovered by the Supplier or the Customer.;

7.5.2 promptly cooperate with any reasonable request for information made in respect of:

- (i) any Incident;
- (ii) any of the information reasonably required;
- (iii) any requests for information, or inspection, made by a regulator with competent jurisdiction over the Customer.

7.6 In the event of any loss or damage to Customer Data, the Customer's sole and exclusive remedy shall be for the Supplier to use reasonable commercial efforts to restore the lost or damaged Customer Data from the latest backup of such Customer Data maintaine d by the Supplier in accordance with the archiving procedure described in the Managed Services Description. The Supplier shall not be responsible for any loss, destruction, alteration or disclosure of Customer Data caused by any third party (except those t hird parties subcontracted by the Supplier to perform services related to Customer Data maintenance and back-up).

8. WARRANTIES

8.1 The Supplier warrants, represents and undertakes that:

8.1.1. it has the full capacity and authority to enter into and perform this schedule and that this schedule is executed by a duly authorised representative of the Supplier;

8.1.2 it owns, or has obtained valid licences, consents, permissions and rights to enable the Supplier to comply with this schedule and to use any of the Intellectual Property Rights necessary for the fulfilment of all its obligations under this schedule including for the Customer’s use and receipt of the Services, and the Supplier shall not breach the provisions of any such necessary licences, consents, permissions and rights or cause the same to be breached;

8.1.3 it shall comply with all applicable laws and regulation (applicable at the date of this schedule) in performing its obligations under this schedule. For the avoidance of doubt unless specifically stated in these terms this does not include any heightened cybersecurity requirements to which the Customer may be subject under the European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 (S.I. No. 360 of 2018) or any legislation implementing Directive (EU) 2022/2555 (NIS2) in Ireland;

8.1.4 the Customer’s possession and use in accordance with this schedule of any materials (including third -party materials) supplied by the Supplier to the Customer shall not cause the Customer to infringe the rights, including any

Intellectual Property Rights, of any third party;

8.1.5 any software, system or telecommunications provided by or on behalf of the Supplier shall be tested for Viruses, Known Vulnerabilities and any of the same that are identified shall be Mitigated against before the date of delivery or use of such software, systems or telecommunications by the Supplier; and

8.1.6 all personnel and sub -contractors used by the Supplier in the performance of this schedule are adequately skilled and experienced for the activities they are required to perform; and

8.1.7 it will make all reasonable efforts not to introduce, or permit the introduction of, any Viruses or Known Vulnerabilities into Customer’s Operating Environment, or the Customer’s other network and information systems, while performing the Services.

8.2 Without prejudice to express warranties contained in this schedule, all implied warranties and representations (including without limitation any warranty or representation that the Service is free of defects, of satisfactory quality, or fit for a particul ar purpose) relating to the Managed Services are hereby excluded.

8.3 Where the Supplier agrees to retain and manage Inherited Technology, responsibility for that item shall transfer to the Supplier only from the date on which the item is recorded in the agreed asset register or Managed Services Description, the

Supplier has completed any required assessment and remediation, the Customer has accepted any documented residual risks, and the Supplier has confirmed acceptance in writing.

9. CHARGES AND PAYMENT

9.1 The Customer shall pay the Managed Services Fees made up of the Set-Up Services Fees and the Monthly Fees, Maintenance Services Fees (if any).

9.2 The Customer shall also pay for any Additional Services.

9.3 The Customer shall also reimburse the Supplier for all actual, reasonable travel costs and expenses including airfares, hotels and meals incurred by the Supplier in performance of the Set-up Services. Any reimbursement shall be subject to prior written consent from the Customer.

9.4 The Managed Services Fees shall be invoiced in the following manner:

9.4.1 The Supplier shall invoice the Customer for the Set -Up Services and the Customer shall pay to the Supplier the Set-Up Services Fees as set out in the Acknowledgement prior to the Set-Up Services being commenced. Any delay in the payment of the Set -Up Services Fees shall entitle the Supplier to delay the Set-Up Services to such time as the Invoice is satisfactorily paid and the Supplier shall have no liability for this delay.

9.4.2 The Supplier shall invoice the Customer monthly in advance as of the first day of each month for the Monthly Fees, and Maintenance Fees and monthly on the first day of the month for any Additional Services performed by the Supplier during the previous month. If any Service Credits are due then they shall be shown as a deduction from the invoice.

9.6 If the Maintenance Services Fees are not paid on time in accordance with this paragraph 9 the Supplier may at its option suspend the Managed Services part ly or fully for such period as the Charges remain outstanding and if this period fails to remedy the non-payment within thirty (30) days (or such longer period as specified in the appropriate notice) of the receipt by the Customer of a written notice sent by the Supplier which clearly stipulates the payment(s) that have not been made by the Customer and that the Supplier intends to suspend such Managed Services if payment is not received within the specified period. Any such suspension shall be without prejudice to its right to terminate this schedule. Where the Managed Services are suspended under this paragraph 9.10 the Customer will still be liable to pay all Charges until this schedule is terminated. For the avoidance of doubt the suspension of the Services shall be limited to those Managed Services to which the non-payment relates and not any other Services provided by the Supplier under this Contract.

10. CONTINUOUS IMPROVEMENT

10.1 The Supplier shall, at its own cost and expense, submit a report to the Customer from time to time identifying the emergence of new and evolving relevant technologies or process changes in the IT, telecommunications or data centre field relevant to the Managed Services. Such report shall be provided in sufficient detail to enable the Customer to evaluate properly the benefits of the new technology or process.

10.2 If the Customer wishes to incorporate any improvement identified by the Supplier under Paragraph 10.1 , the Customer shall send the Supplier a change request for consideration in accordance with the General Terms.

11. SERVICE REVIEW AND GOVERNANCE

11.1 The Customer’s Project Manager and the Supplier’s Project Manager shall have regular meetings (Quarterly Meetings) to monitor and review the performance of this schedule, to discuss any changes and to discuss the Service Level Arrangements. These meetings shall be minuted by the Supplier’s Project Manager and copies of those minutes shall be circulated to, and approved by, both parties.

11.2 Before each Monthly Meeting, the Customer’s Project Manager shall notify the Supplier’s Project Manager, and vice versa, of any problems relating to the provision of the Services for discussion at the Quarterly Meeting. At each such meeting, the parties shall agree a plan to address such problems. In the event of any problem being unresolved or a failure to agree on the plan, the matter shall be resolved in accordance with as a dispute under the General Ters. Progress in implementing the plan shall be included in the agenda for the next Quarterly Meeting.

11.3 A review meeting to assess the performance of the Supplier in the delivery of the Managed Services shall be held instead of the fourth Quarterly Meeting (Review Meeting). Each Review Meeting shall be attended by senior representatives of the Customer and of the Supplier, together with the Customer’s Project Manager and Supplier’s Project Manager.

11.4 The Customer and the Supplier shall review the Service Level Arrangement at each Review Meeting and shall, in accordance with Paragraph 6 agree modifications to reflect changes in the Customer’s requirements for the Managed Services.

11.5 Where any of the Assets or Customer's equipment used to provide the Managed Services becomes obsolete in the sole but reasonable opinion of the Supplier (including but not limited to when the manufacturer of such equipment declares it 'end of life' and no longer supports such equipment) the Supplier shall submit to the

Customer a report on the alternative possibilities to replace such Assets/Customer equipment as required. The Customer may either agree to purchase the additional Assets/Customer Equipment under the Change Control procedure (paragraph 6) or shall give notice of termination in accordance with Paragraph 14.2.

12. PROPRIETARY RIGHTS

12.1 Nothing in this schedule affects either party's rights in pre-existing Intellectual Property Rights (including pre-existing Intellectual Property Rights of either party contained in or relating to Confidential Information) (Pre-Existing IPR).

12.2 The Customer acknowledges such title, interest and rights and the Customer shall not take any action to jeopardise, limit or interfere in any manner with the Supplier's (or any third party suppliers) title, interests or rights with respect to the Managed s ervice including but not limited to using the Supplier's trademarks or tradename.

12.3 The Supplier acknowledges and agrees that the Customer owns and retains all rights, title and interest in and to the Customer Data. The Supplier shall have no rights to access, use or modify the Customer Data unless it has the prior written consent of the Customer.

12.4 The Customer acknowledges and agrees that the Customer shall have no rights to any intellectual property rights arising as a result of the use of the Managed Services or developed during the Managed Services except for a licence, as stated in paragraph

12.4 below, to use the Supplier's intellectual property solely to the extent necessary for the provision of the Managed Services.

12.5 The Supplier grants to the Customer solely for the term of this schedule a revocable, sub-licensable, non-transferable, non-exclusive, royalty-free, worldwide limited licence to use and sub -license to guests, all of the Supplier's Intellectual Property Rights as incorporated by the Supplier into the Work Product solely in connection with the Customer's (and its permitted sub-licensees') use of the Work Product in accordance with this schedule.

12.6 The Customer grants to the Supplier a revocable, sub -licensable, non-transferable, non-exclusive, royalty-free, worldwide limited licence for the term of this schedule to use, exploit, copy, reproduce, manufacture, sub -license, modify, improve, enhance and make derivative works of the Customer's Intellectual Property Rights solely to the extent necessary to enable the Supplier to comply with its obligations under this schedule.

12.7 The Supplier shall not disclose to the Customer or use in its work any trade secrets or confidential information of a third party which the Supplier is not lawfully entitled to disclose or use in such manner. The Supplier shall not use any equipment, supp lies, facilities, computer code, work product, inventions or materials of any other third party (Third-Party Materials) in any Work Product or in the Supplier's performance under this schedule unless:

12.7.1 the Supplier has the full right and authority to do so without violating any rights of any third party;

12.7.2 the Supplier has obtained all necessary rights to enable it to perform its obligations under this schedule and grant the rights granted pursuant to this schedule, and to permit the Customer to utilise the Third -Party Materials as contemplated under this schedule, in each case at no additional cost or expense to the Customer;

12.7.3 the Customer's use of such Third -Party Materials will not restrict or impair in any manner its use of the Work Product or subject the Customer to any obligation or liability; and

12.7.4 such Third-Party Materials are specifically identified to the Customer in writing in advance of any use and the Customer has agreed in writing to such use.

12.8 The Supplier grants to the Customer or the term of this schedule an, irrevocable, sub- licensable, non-transferrable, non-exclusive, royalty-free, worldwide licence to such Third-Party Materials as are incorporated in the Work Product solely in connection with the Customer's (and its permitted sub -licensees') use of the Wo rk Product in accordance with this schedule.

12.9 For the avoidance of doubt the Customer-site Equipment shall remain the property of the Supplier or the supplier of such equipment and the Customer shall at all times make clear to third parties that the same is the property of the Supplier or a third -party supplier of the Supplier.

12.10 Each party reserves all rights not expressly granted in this schedule.

13. LIMITATION OF LIABILITY

In addition to the Limitations of Liability set out in the General Terms the Supplier further limits their liability, subject always to Paragraph 14.4 of the General Terms, in the following way:

13.1. The Service Level Arrangements state the Customer's full and exclusive right and remedy, and the Supplier's only obligation and liability, in respect of the performance and availability of the Managed Services, or their non -performance and non - availability.

13.2 Service credits shall be limited in accordance with the SLA.

13.3 INHERITED TECHNOLOGY AND CYBER AND DATA LIABILITY

13.3.1 Subject to paragraph 13.3.4, the Supplier shall not be liable for any loss, damage, corruption, interruption, security incident, personal-data breach or unauthorised access to the extent caused or contributed to by Inherited Technology or an Inherited Vulnerability; an act or omission of a previous managed service provider, incumbent supplier or other third party occurring before the Commencement Date; the Customer's failure to provide complete information, access, credentials or authority; the Customer's or a third party's delay or refusal in implementing recommended remediation; or Inherited Technology that the Customer instructs the Supplier not to remove, disable, replace or remediate.

13.3.2 Receipt of system access, monitoring alerts, administrative credentials or information relating to Inherited Technology shall not by itself constitute acceptance of responsibility for that technology or any associated vulnerability.

13.3.3 The exclusions in this paragraph shall not apply to the extent that the relevant loss was directly caused by the Supplier introducing the vulnerability after the Commencement Date, materially worsening an Inherited Vulnerability, failing to take reasonable steps after identifying and accepting responsibility for the vulnerability, or by liability that cannot lawfully be excluded.

13.3.4 To the fullest extent permitted by law and subject only to Non-Excludable Liabilities, the Supplier's total aggregate liability to the Customer arising out of or in connection with all Cyber and Data Events shall not exceed the total Managed Services Fees paid or payable by the Customer under the affected Managed Services Schedule during the twelve months immediately preceding the first Cyber and Data Event giving rise to liability. Where an event occurs during the first twelve months, the cap shall be the Managed Services Fees paid or payable from the Commencement Date to the date of the event, annualised over twelve months.

13.3.5 The cap applies collectively to all liability arising in contract, tort including negligence, breach of statutory duty, misrepresentation, restitution, indemnity or otherwise, and to damages, compensation, indemnity payments, remediation costs, restoration costs, investigation costs, notification costs and other amounts claimed by the Customer.

13.3.6 All Cyber and Data Events arising from the same or related vulnerability, incident, act, omission, underlying cause or series of events shall be treated as one event and one claim regardless of the number of affected systems, users, data subjects, claims or claimants.

13.3.7 The Customer's sole and exclusive contractual remedies for a Cyber and Data Event shall be the Supplier's use of reasonable commercial endeavours to contain and remediate the incident; restoration of Customer Data from the latest available usable backup included within the Managed Services; applicable Service Credits; and damages recoverable within the aggregate cap in paragraph 13.3.4.

13.3.8 The Supplier shall not be liable for loss of profit, revenue, business, contracts, anticipated savings, goodwill or reputation; loss or corruption of data except for reasonable restoration from an available backup; business interruption; the cost of recreating data; or indirect or consequential loss.

13.3.9 The aggregate cap shall not be multiplied by the number of duties breached, causes of action, affected systems, affected individuals, claims, claimants or policy periods.

13.3.10 Nothing in this paragraph limits liability for death or personal injury caused by negligence, fraud or fraudulent misrepresentation, deliberate default or any other liability that cannot lawfully be limited or excluded (Non-Excludable Liabilities). This paragraph allocates liability solely between the Supplier and the Customer and does not restrict the rights of a regulator or person who is not a party to the Contract.

13.3.11 This paragraph takes precedence over any inconsistent liability provision in the General Terms in respect of a Cyber and Data Event.

14. TERM AND TERMINATION

14.1 This schedule shall commence on the Commencement Date. Unless terminated earlier in accordance with this Paragraph 14, this schedule shall continue in force for the Initial Term and shall automatically extend for successive 12 - month periods (

Extended Term) at the end of the Initial Term and at the end of each Extended Term. A party may give written notice to the other party, not later than 90 days before the end of the Initial Term or the relevant Extended Term, to terminate this schedule at the end of the Initial Term or the relevant Extended Term, as the case may be.

14.2 Without prejudice to any rights that have accrued under this schedule or any of its rights or remedies and subject to Paragraph 15, the Customer may terminate this schedule before the end of the Initial Term or Extended Term (as the case may be) on giving not less than 90 days written notice to the Supplier, provided that on any such termination it shall, without prejudice to any accrued rights or obligations as at that time, be obliged to pay termination compensation to the Supplier calculated as stated in paragraph 14.6.1 below:

14.3 Without prejudice to any other right or remedy available to it, and subject to Paragraph

14.6 and 15, either party may terminate this schedule with immediate effect by giving written notice to the other party if:

14.3.1 for any reason which the party is entitled to under the General Terms Paragraphs 16; and

14.3.2 in the case of a due diligence exercise on an existing Customer Operating Environment where it transpires that the Customer Operating Environment is insufficient and either the Customer does not wish to upgrade the system or the Supplier has not been able to improve the Customer Operating Environment to a sufficient degree to reasonably allow use in accordance with this schedule;

14.3.3 in the case of Maintenance being undertaken that requires Additional Services and the Customer/Supplier does not wish to proceed with the Managed Services;

14.3.4 Where the Supplier increases their Charges by more than 10% following a survey conducted under Paragraph 2.3 and the Customer does not wish to continue with the Managed Service

14.4 Without prejudice to any other right or remedy available to it, and subject to Paragraph 15, the Supplier may terminate this schedule immediately on notice where there is a change of control of the Customer (within the meaning of section 11 of the Taxes Consolidation Act 1997).

14.5 Without prejudice to any other right or remedy available to it, and subject to Paragraph 15, the Supplier may terminate this schedule with immediate effect by giving written notice if the Customer breaches any material terms of the Data Protection requirements of the General Terms or the security provisions in Paragraph 6.

14.6 Termination payments shall be paid by the Customer to the Supplier in respect of the following paragraphs in the respective amounts:

14.6.1 Termination under Paragraph 14.2 the payment of 100% of the remaining Fees until the end of the Initial Term or Extended Term as the case may be,

14.6.2 Termination in accordance with Paragraph 14.3.2 or 14.3.3 : A payment in respect of the due diligence exercise;

14.6.3 Termination in accordance with Paragraph 14.3.4: A payment of €1,000 in respect of the survey.

14.7 The party not affected by a continuing Force Majeure Event may terminate this schedule in accordance with the General Terms provisions for Force Majeure.

14.8 Any provision of this schedule which expressly or by implication is intended to come into or continue in force on or after expiry or termination of this schedule shall remain in full force and effect.

14.9 Termination of this schedule for any reason shall not affect the accrued rights, remedies, obligations or liabilities of the parties existing at expiry or termination.

14.10 On expiry or termination of this schedule for any reason:

14.10.1 the Supplier shall immediately cease provision of the Set -Up Services, Managed Services and Maintenance Services but shall provide Transition Services for a further period in accordance with Paragraph 15.2;

14.10.2 (subject to Paragraph 14.10.1) each party shall make no further use of any equipment, property, materials and other items (and all copies of them) belonging to the other party and the Customer shall cease to use any IP address licensed to the Customer by the Supplier pursuant to Paragraph 15.3; and

14.10.3 The Customer shall, at its expense return all Customer -site Equipment to the Supplier and where this is not returned to the Supplier within 30 days the Supplier shall be charged and shall pay the Fee for the purchase of the Customer-site Equipment.

14.10.4 if the Supplier receives, no later than ten days after the Commencement date of the expiry or termination of this schedule for any reason, a written request for the delivery to the Customer of the most recent backup of the Customer Data and such request is, where relevant, in accordance with Paragraph 7.4 the Supplier shall use reasonable commercial endeavours to deliver the backup to the Customer within 30 days of its receipt of such a written request in the format stored or in a format as otherwise reaso nably requested by the Customer, provided that the Customer has at that time paid all Charges outstanding at (and including any resulting from) expiry or termination (whether or not due at the date of expiry or termination). Once such ten -day period has expired or the Supplier has, at the Customer's request, delivered to the Customer the most recent backup of the Customer Data (as applicable), the Supplier shall (subject to Paragraph 14.10 .1) promptly expunge from the Supplier's System and otherwise destroy or dispose of all of the Customer Data in its possession or control. The Supplier shall bear all reasonable costs and expenses incurred in returning and disposing of Customer Data and expunging it from the Supplier's system.

14.11 If a party is required by any law, regulation, or government or regulatory body (Regulatory Requirement) to retain any documents or materials which it would otherwise be obliged to return or destroy under Paragraph 14.10), it shall notify the other party in writing of such retention, giving details of the documents or materials that it must retain. Paragraph 12 and confidentiality under the General Terms shall continue to apply to any such retained documents and materials for as long as any such requirement continues in force, subject to any disclosure mandated by any Regulatory Requirement.

15. EXIT ASSISTANCE AND TRANSFER OF ASSETS

15.1 The Supplier shall, on request from the Customer at any time after the expiry of six months from the Acceptance Date, prepare for the orderly transition of the Services from the Supplier to the Customer or its nominated Replacement Supplier by provision of the necessary credentials to the Customer.

15.2 The Customer may, at any time before expiry or termination of all or any part of this schedule for any reason request the Supplier to provide the Transition Services or otherwise to offer reasonable assistance in transitioning the Services to the Customer or a Replacement Supplier (by providing the Transition Services). The Supplier shall, in consideration of a reasonable fee (to be agreed in advance), provide such Transition Services for a maximum period of three months, or until expiry or terminati on of all or any part of this schedule for any reason in accordance with Paragraph 14, whichever is later.

15.3 The Supplier and Customer shall co-operate to procure the novation or assignment to the Customer and/or Replacement Supplier of the Transferring Contracts.

15.4 The Customer shall:

15.4.1 accept assignments from the Supplier at the Customer's sole discretion, otherwise join with the Supplier in procuring a novation of each Transferring Contract; and"

15.4.2 once a Transferring Contract is novated or assigned to the Customer or the Replacement Supplier, carry out, perform and discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract or, as applicable, procure that the Replacement Supplier does the same.

16. Non-solicitation of employees or contractors

16.1 In order to protect the legitimate business interests of the Supplier, the Customer covenants with the Supplier that it shall not (and shall procure that no member of the Customer's group) shall (except with the prior written consent of the Supplier):

- (a) attempt to solicit or entice away; or
- (b) solicit or entice away,

from the employment or service of the Supplier the services of any Restricted Person other than by means of a national advertising campaign open to all -comers and not specifically targeted at such staff of the Supplier.

16.2 The Customer shall be bound by the covenant set out in clause 16.1 during the term of this schedule, and for a period of 6 months after termination of this schedule.

16.3 For the purposes of this clause 16, a Restricted Person shall mean any firm, company or person employed or engaged by the Supplier during the term of this Contract, who has been engaged in the provision of the Services or the management of this schedule either as principal, agent, employee, independent contractor or in any other form of employment or engagement.

Non-employment of employees

17.1 In order to protect the legitimate business interests of the Supplier, the Customer covenants with the Supplier that it shall not (and shall procure that no member of the Customer's group shall) (except with the prior written consent of the Supplier) employ or engage or otherwise facilitate the employment or engagement of any Restricted Person.

17.2 The Customer shall be bound by the covenant set out in clause 17.1 during the term of this schedule and for a period of 6 months after termination of this schedule.

17.3 For the purposes of this clause 17, a Restricted Person shall mean any firm, company or person employed or engaged by the Supplier during the term of this schedule, who has been engaged in the provision of the Services or the management of this schedule either as principal, agent, employee, independent contractor or in any other form of employment or engagement.

18. GOVERNING LAW AND JURISDICTION

18.1 This schedule and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non -contractual disputes or claims) shall be governed by and construed in accordance with the law of Ireland.

18.2 Each party irrevocably agrees that the courts of Ireland shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this schedule or its subject matter or formation (including non -contractual disputes or claims).

This schedule has been entered into on the date stated in the Acknowledgement

Sub Schedule 1 Managed Services Implementation

1. PLANNING AND DUE DILIGENCE

The Supplier shall prepare the Project Plan in co -operation with the Customer. Where the Set-Up Services include the taking over of a previously non -Supplier installed system The Project Plan shall list the detail in respect of the service currently in place and give the Supplier the reasonable information on the existing system as required in accordance with this schedule and a due diligence exercise shall be undertaken by the Supplier to see whether the Customer Operating Environment is suitable for the provision of the Managed Services.

2. IMPLEMENTATION

The Supplier and the Customer shall co -operate in implementing the Managed Services in accordance with the implementation provisions of the Project Plan.

3. ROLL-OUT

The Supplier and the Customer shall co -operate in rolling out the Managed Services in accordance with the roll-out provisions of the Project Plan.

4. MINIMUM STANDARDS REQUIRED FOR THE SERVICES

In order for the Customer’s existing environment to qualify for the Suppliers Managed Service the following requirements must be met:

- (a) All Servers and endpoints with Microsoft Windows Operating Systems must be running software versions that are within Microsoft’s ‘extended support dates’.
- (b) All server and desktop software must be genuine, licensed and vendor Supported.
- (c) The environments must have a vendor supported backup solution that can be monitored and send notifications on job failures and successes.
- (d) The environments must have a currently licenced vendor supported hardware firewall between the Internal Network and the Internet.

5. EXCLUDED SERVICES

Services rendered under this Schedule do not include:

- (a) Parts, equipment or software not covered by vendor/manufacture warranty or support.
- (b) The costs of shipping charges of any kind.
- (c) The costs of any software, licensing or software renewal or upgrade fees of any kind.
- (d) The cost of any third-party vendor or manufacturer support or incident fees of any kind.
- (e) The cost to bring the Customer’s environment up to the minimum standards required for Services.
- (f) Failure due to acts of God, building modifications, power failures or other adverse environmental conditions or factors.

- (g) Service and repairs made necessary by the alterations or modifications of equipment other than that authorised by the Supplier including alterations made by the Customer’s employees or anyone other than the Supplier.

SUB-SCHEDULE 2

MANAGED SERVICES DESCRIPTION

The Managed Services Specification is described in the RACI tables below RACI Definition for IT Managed Services R - Responsibility Supplier Customer or 3rd Party Designate A - Accountability C- Consult I - Inform

Support Services Service Desk Facilities Internal support database which holds customer' technical information, systems configuration and network

R I

System that holds customer' asset register with the ability to provide notification of both hardware reaching end of manufacturer or 3rd party warranty period and software licence renewals

R I

Access control tools to allow remote system diagnostics and repair R

Access to technical support centres, databases, patches and software version updates R

Strategic support arrangements with key technology partners e.g. Microsoft, HP etc. A

Incident logging mechanisms via phone, e-mail and/or user portal R

Incident logging database to track incident status and resolution in line with SLA's R

Ability to produce cause, issue and resolution statistics R

Internal incident escalation process R

Escalation management of 3rd Parties where:

- The 3rd Party SLA has been breached - The issue is not being addressed or resolved in an acceptable or timely manner - Mediation is required where multiple suppliers have involvement

R I

Provision of out-of-hours support for the reporting of business critical outages and issues defined as a Priority 1 in the Service Level Agreement R

Existing relationships/contacts with 3rd Party Industry support vendors and full understanding/knowledge of the management of their operating environment:

Property Management Systems R I WAN Systems R I Sales & Catering Systems R I Point of Sale Systems R I Call Accounting & Voicemail Systems R I Operating Systems R I

Financial Accounting Systems R I Door Access Control Systems R I GRE Systems R I Credit Card Systems R I Spa & Golf Systems R I Incident Management Provide initial incident management for all infrastructure hardware and software related issues R

Accept Inbound issue calls, emails and portal requests, and log appropriate service tickets within agreed SLA time limits R

Assign priority as per agreed SLA R I Communicate status and resolution of the service ticket to the end user R

Log and escalate to appropriate resource R

Escalate to 3rd Party supplier when applicable and monitor progress through to resolution

R I

System Operations Support services to cover agreed Domain, File & Print, Mail and Application Servers R

Support services to cover all agreed Firewalls, Network Switches and Routers R

Support services to cover all agreed PC's, Laptops and authorised Mobile devices R

Identify & apply operating system updates, patches and fixes R

Perform root cause analysis for major incidents or outages R I Inform customer of scheduled system maintenance R I Monitor and manage RMM alert events R I Perform support, administration and troubleshooting R Determine optimal performance settings for application in supported environments

R I

Identify requirements for new versions and/or new releases R C Image capture where appropriate R

Have disaster recovery process and plan in place R C Ensure emergency manual procedures are in place for critical applications

R Desktop Setup Application access R

Outlook/E-Mail client configuration R

Internet Access configuration R

Authorised mobile device e-mail support R I Printer mapping R

Drive mapping R

Restricted access inline with Group permission R R Desktop lockdown & unauthorised software installation/access R C Standardised provisioning of desktop environment R User/Service Request Management Facilitate new user creation in line with customer' user rights and groups policy R I Facilitate account disable/user deletion R I Manage user account changes R I Qualify & support physical moves & changes eg printer/desktop moves C I Perform user password resets R I Add & remove members to/from Distribution lists R Administer Global Address List R Administer Public Folders R Administer Permissions R Client configuration advice R C Define, Implement and maintain System Policies R C Maintain user profile templates R C Identify end-user performance issues R I Administer Active Directory Services (DNS, WINS, DHCP etc.) R I Administer Group Policy R I Network Operations Analyse system health and network activity events R

Network troubleshooting and fault isolation R

Diagnosis of 3rd Party WAN connectivity R

Security Ensure all applicable devices have endpoint Anti-virus installed R I Maintain Anti-virus Definition updates across all applicable devices R

Ensure users have Mail security where applicable R I Maintain Mail security updates for all users R

Detect and maintain virus eradication procedures on all applicable devices R

Manage and monitor Web access, security and control where applicable R I Define Password Rotation Policy C R Implement Password Rotation policy R I Ensure Network security and maintain firmware and software updates R I Analyse security incidents and critical events on firewalls R I Monitor and identify critical and security events network wide to detect attacks and malicious network users

R I

Take corrective action to address security vulnerabilities R I

On site computer room physical security C R Storage and Backup Daily backup monitoring and verification R

Co-ordinate recall of required backup media if required R I Perform restore of data from backup media/ cloud R C Licence Compliance and Renewal (Media, Keys, 3rd Party Maintenance) Devices R A User CALs R A MS Office R A Server Operating Systems R A Server Software e.g. Small Business Server, Virtualisation Software etc. R A Endpoint Anti-virus R A Mail security - Anti-virus/Anti-spam R A SSL Certificates R A Firewall R A Monitoring Software R A Backup Software R A Other Infrastructure Licences as requested R C

RACI Definition for Telephony Support Services R - Responsibility Supplier Customer or 3rd Party Designate A - Accountability C-Consult I - Inform

Support Services Service Desk Facilities Internal support database which holds customer' technical information, systems configuration and network

R I

System that holds customer' asset register with the ability to provide notification of both hardware reaching end of manufacturer or 3rd party warranty period and software licence renewals

R I

Access control tools to allow remote system diagnostics and repair R

Access to technical support centres, databases, patches and software version updates R

Strategic support arrangements with key technology partners A

Incident logging mechanisms via phone, e-mail and/or user portal R

Incident logging database to track incident status and resolution in line with SLA's R

Ability to produce cause, issue and resolution statistics R

Internal incident escalation process R

Escalation management of 3rd Parties where:

- The 3rd Party SLA has been breached - The issue is not being addressed or resolved in an acceptable or timely manner - Mediation is required where multiple suppliers have involvement

R I

Provision of out-of-hours support for the reporting of business critical outages and issues defined as a Priority 1 in the Service Level Agreement R

Existing relationships/contacts with 3rd Party Industry support vendors and full understanding/knowledge of the management of their operating environment:

Telephone Line Providers R I WAN Line Providers R I Call Accounting & Voicemail Systems R I Analogue DECT and SIP DECT providers R I Hosted PABX Providers R I Call Recording Providers R I Analogue handset providers R I Alarm Messaging Systems R I

Incident Management Provide initial incident management for all infrastructure hardware and software related issues R

Accept Inbound issue calls, emails and portal requests, and log appropriate service tickets within agreed SLA time limits R

Assign priority as per agreed SLA R I Communicate status and resolution of the service ticket to the end user R

Log and escalate to appropriate resource R

Escalate to 3rd Party supplier when applicable and monitor progress through to resolution

R I

System Operations Support services to cover all agreed hardware. R

Identify & apply operating system updates, patches and fixes if software assurance is taken as an option and are required to resolve an incident. R

Perform root cause analysis for major incidents or outages R I Inform customer of scheduled system maintenance R I Perform support, administration and troubleshooting R Identify requirements for new versions and/or new releases R C Implement redundant services where in place in the event of a system outage

R C

Ensure emergency manual procedures are in place for disaster recovery

C R

Desktop Setup of Telephony Applications R

Outlook/E-Mail TAPI interfaces R

User/Service Request Management Facilitate new user setup R I Facilitate user deletion R I Manage hunt groups and pick up groups R I Qualify & support physical and remote moves & changes eg phones; voicemail; autoattendent C I Set call permissions

on system Perform user password resets R I Client configuration advice R C Identify end-user performance issues R I Network Operations

Analyse system health and network activity events R

Network troubleshooting and fault isolation R

Diagnosis of 3rd Party WAN / Line connectivity R

Onsite Hardware Cover (where selected by Customer) Replacement of hardware where required: R

Default PABX system hardware covered:

CPU Cards R

Trunk cards R

Analogue cards R

Digital cards R

Consoles R

Embedded voicemail systems R

Listed software applications (e.g. Teleworker; Mitel Border Gateway ;) R

Backup systems R

PMS and SMDR interfaces R

Cabling from the PBX to the TJF/MDF R

System Digital & IP handsets R

EXCLUDED hardware (unless detailed on Service Schedule)

Physical Faults with IP and Digital handsets I R Networking equipment (POE switches; routers etc) I R Analogue handsets I R Third party voicemail systems I R Third party DECT systems I R Wi-Fi DECT solutions I R Third party call logging systems I R Software upgrades on the PABX CPU I R Cabling from the MDF to the sockets I R PC and server hardware for telephony applications I R Third party call recording I R Customer to renew hardware warranty cover where recommended by Penny Apples

C R

Damage due to misuse, tamper, vandalism, failure to maintain necessary environmental conditions or relocation of equipment.

I A

Security Ensure Network security and maintain firmware and software updates where software assurance is in place.

R I

Monitor and identify critical and security events network wide to detect attacks and malicious network users

R I

Take action to address security vulnerabilities and harden the system where possible

R I

Restrict impact of toll fraud by implementing call capping when agreed limits are breached.

R C

On site computer room physical security C R Licence Compliance and Renewal (Media, Keys, 3rd Party Maintenance) Firewall R A Other Infrastructure Licences including Software Assurance R C

RACI Definition for Security Support Services R - Responsibility Supplier Customer or 3rd Party Designate A - Accountability C-Consult I - Inform

Support Services Service Desk Facilities Internal support database which holds customer' technical information, systems configuration and network

R I

System that holds customer' asset register with the ability to provide notification of both hardware reaching end of manufacturer or 3rd party warranty period and software licence renewals

R I

Access control tools to allow remote system diagnostics and repair R

Access to technical support centres, databases, patches and software version updates R

Strategic support arrangements with key technology partners e.g Salto; Hikvision A

Incident logging mechanisms via phone, e-mail and/or user portal R

Incident logging database to track incident status and resolution in line with SLA's R

Ability to produce cause, issue and resolution statistics R

Internal incident escalation process R

Escalation management of 3rd Parties where:

- The 3rd Party SLA has been breached - The issue is not being addressed or resolved in an acceptable or timely manner - Mediation is required where multiple suppliers have involvement

R I

Provision of out-of-hours support for the reporting of business critical outages and issues defined as a Priority 1 in the Service Level Agreement R

Existing relationships/contacts with 3rd Party Industry support vendors and full understanding/knowledge of the management of their operating environment:

Property Management Systems R I Door Access Control Systems R I IT Infrastructure Service Provider R I PABX Support Service Provider R I Mechanical & Electrical Systems Provider R I CCTV System provider R I Incident Management

Provide initial incident management for all infrastructure hardware and software related issues R

Accept Inbound issue calls, emails and portal requests, and log appropriate service tickets within agreed SLA time limits R

Assign priority as per agreed SLA R I Communicate status and resolution of the service ticket to the end user R

Log and escalate to appropriate resource R

Escalate to 3rd Party supplier when applicable and monitor progress through to resolution

R I

System Operations Support services to cover all agreed hardware R

Identify & apply operating system updates, patches and fixes R

Perform root cause analysis for major incidents or outages R I Inform customer of scheduled system maintenance R I Perform support, administration and troubleshooting R Have disaster recovery process and plan in place C R Customer to hold recommended spares package C R Ensure emergency manual procedures are in place C R

User/Service Request Management Facilitate new user creation in line with customer' user rights and groups policy R C Facilitate account disable/user deletion R C Manage user account changes R C Qualify & support physical moves & changes R C Perform user password resets R C Add & remove members R Client configuration advice C R Define, Implement and maintain System Policies C R Identify end-user performance issues R I Network Operations Analyse system health and network activity events R

Network troubleshooting and fault isolation R

Diagnosis of 3rd Party WAN connectivity R

Onsite Hardware Cover (where selected by Customer) Replacement of hardware where required: R

Default system hardware covered:

CCTV Cameras R

CCTV DVR/NVR R

System Power Supplies R

Portable Programming devices R

Card Encoders R

Online door controllers R break glass units R push to exit units R intercoms if part of access control system R

Salto Energy Saving Device R

Salto door locks R

EXCLUDED hardware (unless detailed on Service Schedule)

Networking equipment (POE switches; routers etc) I R Electric door locking mechanism (maglocks; electric strike etc) I R Cabling unles specified I R Lock batteries or other related consumables I R Server or Workstation hardware I R Problems caused by external factors such as door alignment issues or weather damage.

I R

Software updates I R Customer to renew hardware warranty cover where recommended by Penny Apples

I R

Damage due to misuse, tamper, vandalism, failure to maintain necessary environmental conditions or relocation of equipment.

I R

Annual Preventative Maintenance visits (where selected by customers) APM will include battery tests. (Any batteries replaced will be charged for). R I Battery lock check of alignment, functionality and privacy function. R I Check energy saving device (ESD) R I Check of all headend equipment including server, PPD and encoders

R I

Check of maintenance stock R I Check date and times in system R I Check PMS interface operation R I Check that manual backup system pack has been produced and location is known

R I

Provide employee printout and review with the system manager R I Carry out staff training as required R I Check hotel has the correct support contact information R I

Check and clean CCTV cameras and check DVRs for any performance related issues.

R I

Check DVRs for any performance related issues. R I Produce service report with list of outstanding issues and actions R I Security Ensure Network security and maintain firmware and software updates

R I

Take corrective action to address security vulnerabilities R I On site computer room physical security C R Storage and Backup Daily backup monitoring and verification (where Penny Apples has access to server) R

Perform restore of data from backup media/ cloud R C Licence Compliance and Renewal (Media, Keys, 3rd Party Maintenance) Monitoring Software R A Backup Software R A Other Infrastructure Licences as requested R C

RACI Definition for WiFi Support Services R - Responsibility Supplier Customer or 3rd Party Designate A - Accountability C-Consult I - Inform

Support Services Service Desk Facilities Internal support database which holds customer' technical information, systems configuration and network

R I

System that holds customer' asset register with the ability to provide notification of both hardware reaching end of manufacturer or 3rd party warranty period and software licence renewals

R I

Access control tools to allow remote system diagnostics and repair R

Access to technical support centres, databases, firmware version updates R

Strategic support arrangements with key technology partners A

Incident logging mechanisms via phone, e-mail and/or user portal R

Incident logging database to track incident status and resolution in line with SLA's R

Ability to produce cause, issue and resolution statistics R

Internal incident escalation process R

Escalation management of 3rd Parties where:

- The 3rd Party SLA has been breached - The issue is not being addressed or resolved in an acceptable or timely manner - Mediation is required where multiple suppliers have involvement

R I

Provision of out-of-hours support for the reporting of business critical outages and issues defined as a Priority 1 in the Service Level Agreement R

Existing relationships/contacts with 3rd Party Industry support vendors and full understanding/knowledge of the management of their operating environment:

Property Management Systems R I WAN Systems R I GRE Systems R I Incident Management Provide initial incident management for all infrastructure hardware and software related issues R

Accept Inbound issue calls, emails and portal requests, and log appropriate service tickets within agreed SLA time limits R

Assign priority as per agreed SLA R

Communicate status and resolution of the service ticket to the end user R

Customer to co-operate with Penny Apples in performing the Support and provide assitance or information as reasonably required by Penny Apples

I R

Log and escalate to appropriate resource R

Issue is identified as relating to a technical issue with an end user device.

I R

Issue identified as relating to a technical issue with a third party eg internet connection and monitor progress through to resolution

R I

Supply to Penny Apples all information necessary to raise faults with third parties

C R

Unscheduled network configuration changes & amendments for specific events or situations (eg conferences & events)

C I

System Operations Support services to cover all agreed Gateways, Network Switches and Access Points. R

Identify & apply firmware updates as required R

Perform root cause analysis for major incidents or outages R I Inform customer of scheduled system maintenance R I Perform support, administration and troubleshooting R Determine optimal performance settings in supported environments R I

User/Service Request Management Qualify & support physical moves & changes ie Access points / switches C I Identify end-user performance issues R I Network Operations Analyse system health and network activity events R

Network troubleshooting and fault isolation R

Diagnosis of 3rd Party WAN connectivity R

Onsite Hardware Cover (where selected by Customer) Replacement of hardware installed by Penny Apples where required including; Routers; Gateways; POE switches & SFPs; Access Points R

Customer to renew hardware warranty cover where recommended by Penny Apples

C R

Exclusions: faults with routers if internet is provided by a third party I R Exclusions: PCs for business desk if provided by third party I R Exclusions; copper and fibre optic structured cabling problems if installed by third party

I R

Damage due to misuse, tamper, vandalism, failure to maintain necessary environmental conditions or relocation of equipment.

I A

Security Ensure Network security and maintain firmware and software updates

R I

Analyse security incidents and critical events on firewalls R I Monitor and identify critical and security events network wide to detect attacks and malicious network users

R I

End users access to the internet through the Services is in accordance with any applicable terms of use

I R

Penny Apples may be required by law to provide assistance to law enforcement, governmental agencies and other authorities.

R I

Take corrective action to address security vulnerabilities R I On site computer room physical security C R

RACI Definition for Connectivity Support Services R - Responsibility Supplier Customer or 3rd Party Designate A - Accountability C- Consult I - Inform

Support Services Service Desk Facilities Internal support database which holds customer' technical information, systems configuration and network

R I

System that holds customer' asset register with the ability to provide notification of both hardware reaching end of manufacturer or 3rd party warranty period and software licence renewals

R I

Access control tools to allow remote system diagnostics and repair R

Access to technical support centres, databases, patches and software version updates R

Strategic support arrangements with key technology partners A

Incident logging mechanisms via phone, e-mail and/or user portal R

Incident logging database to track incident status and resolution in line with SLA's R

Ability to produce cause, issue and resolution statistics R

Internal incident escalation process R

Escalation management of 3rd Parties where:

- The 3rd Party SLA has been breached - The issue is not being addressed or resolved in an acceptable or timely manner - Mediation is required where multiple suppliers have involvement

R I

Provision of out-of-hours support for the reporting of business critical outages and issues defined as a Priority 1 in the Service Level Agreement R

Existing relationships/contacts with 3rd Party Industry support vendors and full understanding/knowledge of the management of their operating environment:

Telephone Line Providers R I WAN Line Providers R I Incident Management Provide initial incident management for all connectivity related issues R

Accept Inbound issue calls, emails and portal requests, and log appropriate service tickets within agreed SLA time limits R

Assign priority as per agreed SLA R I

Communicate status and resolution of the service ticket to the end user R

Log and escalate to appropriate resource R

Escalate to 3rd Party supplier when applicable and monitor progress through to resolution

R I

System Operations Support services to cover supplied telephone lines R

Support services to cover supplied data connectivity R

Perform root cause analysis for major incidents or outages R I Inform customer of scheduled system maintenance R I Monitor and manage RMM/PRTG alert events R I Perform support, administration and troubleshooting R Ensure emergency manual procedures are in place for disaster recovery

C R

Network Operations Analyse system health and network activity events R

Network troubleshooting and fault isolation R

Diagnosis of 3rd Party WAN connectivity R

Onsite Hardware Cover (where selected by Customer) Replacement of hardware where required: R

Default system hardware covered:

EXCLUDED hardware (unless detailed on Service Schedule)

Internet Distribution Switch I R ADSL/FTTC Routers I R ADSL/FTTC Modems I R Microfilters I R Customer to renew hardware warranty cover where recommended by Penny Apples

C R

Damage due to misuse, tamper, vandalism, failure to maintain necessary environmental conditions or relocation of equipment.

I A

Security On site computer room physical security C R

Penny Apples Hosted Services Description

Cloud Hosting Environment

- Penny Apples hosting guarantees a 99.9% uptime per calendar month. We will refund one days resource costs for every 43 minute period that your service is unavailable, up to a maximum of 30 days. Penny Apples hosting is responsible for providing network connectivity and infrastructure uptime. We are not responsible for Guest OS and application downtime. All SLA refund requests must be made within 7 days of the end of the calendar month via your account manager. Microsoft SPLA costs are not covered as part of this SLA. Planned maintenance is not part of this SLA. At least 7 days prior notice is given to customers when performing planned maintenance. Duration of the downtime window will be provided with each notice.
- The hosting service is billed for Quarterly in advance

- Windows Server OS licensing included
- Clustered synchronously replicated storage
- Access to Microsoft application licensing through SPLA at additional costs not fixed in this agreement
- To maintain integrity of service for all users in a virtual environment, it may be discovered from time to time that a certain account is not suitable for operation in a virtual environment on our servers. In this instance Penny Apples will contact the account holder to discuss options. Reasons for such action may include, but are not limited to: Sites operating scripts requiring a large amount of CPU or Hard Disk resource etc. If your account continuously uses a high amount CPU usage for example, we may have to help you move elsewhere. This is an unlikely event unless you are using powerful resource using scripts or applications. Any attempts to undermine or cause harm to a server or customer is strictly prohibited. It may result in suspension or termination. If your account information is stolen and abuse is carried out, you are still responsible. This includes if your specific account has an attack, for example, a DOS attack and it uses an excessive amount of server resources.
- No physical equipment will be provided or maintained as part of this agreement.
- We will attempt to provide the services 24 hours a day, 7 days a week for as long as you have paid for them. Sometimes, however, for several reasons the services may be unavailable to you. You must recognize and acknowledge that due to the nature of datacenters technology, occasional unavailability of the services cannot be avoided. Sometimes there are equipment malfunctions. At other times we undertake periodic maintenance procedures or repairs. At other times there are causes beyond our control like power failures, interruption or failure of telecommunication or digital transmission links, hostile network attacks, network traffic and other occurrences. We have not promised to provide you with uninterrupted service; however we will do our best effort in all cases to make sure your virtual machine stays up and running.
- You are allocated a monthly bandwidth allowance. This allowance varies depending on the virtual machine package you purchase. Should your account pass the allocated amount we reserve the right to suspend the account until the start of the next allocation and/or suspend the account until more bandwidth is purchased at an additional fee and/or charge you an additional fee for the overages.

SUB-SCHEDULE 3

SERVICE LEVEL ARRANGEMENTS

1. SERVICE LEVELS

All incidents will be classified using the standard industry practice. This uses the identification of the business impact and urgency to prioritise the incident resolution. Business Impact Definition

1 Multiple sites are unable to work, unable to communicate to

clients or significant revenue will be immediately lost from more than one site;

2 A single site is unable to work, revenue will be lost or VIP or

small group of users are impacted;

3 A user or small group of end users are unable to work. Little

or no revenue will be immediately lost (but may be lost at a later date) Business Urgency Definition

1 Incident must be fixed immediately to prevent impact and

severe reputational loss to the firm

2 Incident must be fixed as soon as possible (perhaps a work

around or other process is available)

3 Incident is not time critical

The severity and overall priority applied to individual calls will be determined based on the Incident priority matrix below Business Impact 1 2 3 Business Urgency

1 P1 Critical

e.g. Network outage covering multiple sites P1 Critical e.g. Security incident for example a virus outbreak P2 High e.g. Email server is down

2 P2 High

e.g. Hosted email system outage P2 High e.g. VIP incident P3 Standard e.g. User laptop or PC issue

3 P3 Standard

e.g. File needs to be restored from backup P4 Minor/Change e.g. Printer queue reconfigurations P4 Minor/Change e.g. new user setup request The Supplier shall determine the priority of any fault in accordance with the following table which also states the Target resolution times and when Status Updates should be expected.

SERVICE

LEVEL

Service Desk 8:00am - 6:00pm Mon - Fri Out of Hours x 365 - P1 Only Priority Example Target Resolution Time Status Updates P1 Critical Security incidents (Virus / Malware Outbreak, Firewall) Full Network Outage (WAN, LAN, Internet, DNS, DHCP, AD) Critical hotel applications and guest systems (PMS, POS, CC, CRS, Wifi, Keycard) 1-hour 24/7 (target 90%)

1 Hour

unless longer duration is mutually agreed P2 High Service Degradation affecting multiple users or properties. Server Outage: Email, File & Print, Scanning. Non-critical hotel applications and systems (Telephony, Call Accounting) Backup / Restore not working VIPs incidents

4 Business

hours (target 90%) 4 hours unless longer duration is mutually agreed P3 Standard Individual user impact with minimal business impact and inconvenience Single user or Laptop/PC issues. Non-critical business applications (Office suite, Adobe) File restore

8 Business

hours (target 90%) Daily unless longer duration is mutually agreed P4 Minor/Change How do I? type calls New user email and login. New user profile setup, user account management, change requests

48 Hours

(target 90%) As mutually agreed If no progress has been made on a Priority 1 or Priority 2 incident within the target resolution time, the incident shall be escalated to the Head of Managed Services. If the incident is not resolved, then after each successive increment of the target resolution time the incident shall be escalated to the Account Director, followed by the Managing Director

A Critical incident can be reduced to a high incident should a workaround (such as failing over

links) be provided, whilst the underlining cause is still being investigated. The timer of the ticket incidence is paused if we are awaiting a customer or third-party supplier response. The timer is also paused if the workaround in place is effective in providing the service whilst the primary service is fixed.

SERVICE CREDITS

In any given month the Customer shall in no event be entitled to receive a Service Credit that exceeds 100% of its monthly Fee for the non-conforming Managed Services. Any Service Credits earned by Customer will be applied to the Managed Services Fees owed by Customer for the next billing period for which the Service Credit applies. The Customer acknowledges and agrees that the terms of this Sub-Schedule 3 relating to Service Credits do not operate by way of penalty and are proportionate when considering the Customer’s legitimate interest to avoid any delay in the provision of the Managed Services

SLA CLAIMS

The Customer shall not be entitled to any Service Credits in respect of the first 30 days of the Service. The Supplier will provide Monthly reporting on Supplier compliance to SLAs no later than five

- (5) business days following the end of the month to which the SLA compliance report applies.

The Customer must notify the Supplier within five (5) business days from receipt of SLA compliance report that it intends to receive a remedy under any one of the SLAs set forth below. Failure to comply with these reporting requirements may forfeit the Customer's right to receive a remedy in connection with an SLA. For all claims subject to validation by the Supplier, the Supplier will use log files, database records, audit logs, and any other information available to validate claims and make a good faith judgment on the applicability of SLAs to said incident. The Supplier shall make information used to validate a SLA claim available for auditing by the Customer at the Customer's request. Except for Material Breach and wilful misconduct, the remedies set forth herein represents the Customer's sole and exclusive remedy for the Supplier's breach of the Service Levels defined in this SLA. If the percentage of overall issues resolved within target falls below 70% for three (3) successive months, this will constitute a Material Breach of this schedule. Exclusions The Customer shall not have any remedies under any SLA to the extent any SLA claim is due to:

- (i) Hardware fault/breakdown where the Supplier has to attend at the Customer Site to make the repair; (ii) The failure or fault in Third Party hardware, services and application issues;
- (iii) The Customer making unauthorised changes to the configuration of affected hardware, software or services;
- (iv) The Customer preventing the Supplier from performing required maintenance and update tasks;
- (v) The issue being caused by unsupported equipment, software or services;
- (vi) The problem being caused by the Customer using equipment, software or service(s) in a way that is not recommended by the Supplier;
- (vii) If Customer is in Breach of the contract with Supplier for any reason (e.g. late payment of Charges);
- (viii) A Force Majeure Event . Remedy Supplier warrants that problem resolution will occur within the problem resolution targets as defined and agreed between Supplier and Customer and documented in the Service Level table for greater than (>) 70% of the Priority 1,2,3 issues logged with Suppl ier Service Desk over a calendar month. For purpose of this SLA the calculation will be

Total Issues Completed During Calendar Month and Resolved Within Target Total Completed Logged During Calendar Month

The Service Credit will be calculated on a per property basis in accordance with the table below.

% Issues Resolved Within Target Service Credit < 70% 25% < 60% 50% < 50% 100%