TERMS AND CONDITIONS FOR THE PROVISION OF IT SERVICES

THIS AGREEMENT is made on

BETWEEN

(1) JUNGLE I.T LIMITED a company incorporated and registered in England and Wales with company number 05008636 having its registered office at Number One, Great Exhibition Way, Kirkstall Forge, Leeds, LS5 3BF ("Supplier");,

(2) Company Name a company incorporated and registered in England and Wales with company number **Company Reg** having its registered office at **Company Address** ("Customer")

BACKGROUND

(A) The Supplier is a provider of Services**.**

(B) The Customer wishes to appoint the Supplier to provide the Services to it in accordance with the terms of this agreement.

AGREED TERMS

1. **DEFINITIONS AND INTERPRETATION**

1.1 The following definitions apply in this agreement, unless the context otherwise requires:

Applicable Laws: any and all (a) legislation including statutes, statutory instruments, regulations, edicts, bye-laws, orders, directives or treaties) and common law; (b) judgments, resolutions, decisions, orders, notices and demands of any court, regulator or tribunal; and (c) rules, policies, guidance or recommendations issued by any governmental, statutory or regulatory body, in each case whether local, national, international or otherwise existing from time to time in any relevant jurisdiction which relates to a party, this agreement and/or the Services.

Available Services: the services available as set out in Schedule 1.

Business Day: any day other than a Saturday, Sunday or a bank or public holiday in England.

Business Hours: the period from 8.00 am to 6.00 pm on any Business Day. Exclusive of scheduled company training.

Change: has the meaning given to it in clause 11.

Confidential Information: any information of whatever nature, that is either identified by the disclosing party as confidential or may be reasonably regarded as confidential by the disclosing party, including documents, letters, plans, diagrams, sketches, drawings, photographs, models, specifications, forecasts, financial information, software, programs, data and any other material bearing or incorporating any information relating to the disclosing party and/or its know-how, business, affairs and/or customers.

Commencement Date: the date of last signature of this agreement,

Customer Materials: all documents, information and materials in any form (including hard copy and electronic form), which are provided by the Customer to the Suppler in connection with the Services.

Data Protection Legislation: in each case to the extent applicable to the parties and as amended or updated from time to time: (i) GDPR; (ii) the UK GDPR; (iii) the Data Protection Act 2018; (iv) the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (v) any other applicable data protection and privacy laws.

Deliverables: any output of the Services to be provided to the Customer as specified in a Service Order and any other documents, products and materials provided by the Supplier to the Customer in relation to the Services (excluding any equipment belonging to the Supplier).

Delivery Location: has the meaning given to it in the Service Order.

Dispute Resolution Procedure: the dispute resolution procedure set out in clause 17.

Documentation: has the meaning given to it in clause 12.

Force Majeure Event: any event or circumstances outside the reasonable control of either party affecting its ability to perform any of its obligations under this agreement (when taking into account that party's responsibility to have resilient systems designed to mitigate common interruptions) including act of God, fire, flood, severe weather, epidemic or pandemic, war, revolution, acts of terrorism, riot or civil commotion, trade embargo, strikes, lock-outs or other industrial action, and interruption of utility service.

GDPR: the General Data Protection Regulation ((EU) 2016/679).

Good Industry Practice: the exercise of that degree of skill, care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced operator engaged in providing services of the same kind as the Services.

Goods: any goods to be sold by the Supplier to the Customer pursuant to an applicable Service Order.
Intellectual Property Rights or IPRs: any current and future intellectual property rights including patents, rights to inventions, business names and domain names, copyright, trade marks, rights in designs, database rights, rights to use, and protect the confidentiality of, confidential information and all other intellectual property rights, whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.

Milestones: a date by which a part of the Services is to be completed, as set out in an applicable Service Order.
Minimum Term: means 36 Months.

Month(s): a calendar month, and months and monthly shall be construed accordingly
Provider's Terms: the standard licensing terms and conditions of the relevant provider/licensor, or the standard terms of supply of the relevant supplier, in respect of a particular re-sold Service (or software).

Renewal Term: has the meaning in clause 2;

Restricted Person: has the meaning given to it in clause 9.1;

Service Order: a detailed plan, agreed in accordance with clause 3, describing the Services to be provided by the Supplier, the timetable for their performance and the related matters listed in the template service order set out in Schedule 2.

Services: the Available Services to be provided by the Supplier to the Customer under this agreement as set out in the Service Order.

Services Start Date: the date the Services are to commence, as detailed in an applicable Service Order.

Service Order Charges: the sums payable by the Customer to the Supplier for the Services and/or Goods (as applicable) as set out in a Service Order.

Specification: the requirements for the Services as set out in Schedule 1, and an applicable Service Order.

Supplier Materials: all documents, information and materials in any form (including hard copy and electronic form), which are provided by the Supplier to the Customer in connection with the Services,

Third Party Software: the software programs proprietary to third parties which are provided to the Customer without modification, with the Deliverables.

UK GDPR: has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

1.2 The Schedules form part of this agreement and shall have effect as if set out in the full body of this agreement. Any reference to this agreement includes the Schedules.

1.3 Any words following the terms including, include, in particular, for example or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms.

2. COMMENCEMENT AND DURATION

2.1 This agreement shall commence on the Commencement Date and shall continue for the Minimum Term, and thereafter automatically extend for 12 Month periods (each 12 Month period a "**Renewal Term**(s)") at the end of each Minimum Term and Renewal Term (as the case may be) unless and until (a) the agreement is terminated earlier in accordance with clause 19, or (b) either party gives to the other party not less than 90 days' written notice to terminate. Such notice to terminate shall be served no earlier than 120 days prior to the end of the Minimum Term or any subsequent Renewal Term(s) (as) applicable, and following such notice the agreement shall terminate on the later of (i) the completion of all Service

Orders entered into before the date on which notice is served; or (ii) the end of the Minimum Term or any subsequent Renewal Term(s) during which the termination notice was provided (as applicable).

2.2 The parties shall not enter into any further Service Orders after the date on which notice to terminate is served under clause 2.1.

2.3 The Customer may procure any of the Available Services and/or Goods (as applicable) by agreeing a Service Order with the Supplier pursuant to clause 3.

2.4 The Supplier shall provide the Services from the date specified in the applicable Service Order.

3. SERVICE ORDERS

3.1 The Customer may at any time ask the Supplier to provide any or all of the Available Services, whereupon the Supplier shall prepare a draft Service Order which the parties shall discuss and seek to agree.

3.2 Where the Service (or any element of it) in the Service Order is identified as a "Re-sold Service", the Service (including without limitation any software supplied pursuant thereto) is re-sold by the Supplier and therefore is provided to the Customer subject to any further provisions in the relevant Provider's Terms, which where possible and if so requested by the Customer, will be provided to the Customer in advance of a Service Order being entered into or made available on a 'click-wrap' or 'shrink-wrap' basis. The Customer acknowledges and agrees that it shall have no greater rights or remedies against the Supplier in respect of a Re-sold Service, as the Supplier has against the provider of the Re-sold Service. The relevant Provider's Terms shall also be deemed to apply as between the Supplier and the Customer to the extent that the obligations or liabilities of the relevant provider are of narrower scope than the obligations or liabilities of the Supplier in this agreement (or as may be otherwise implied).

3.3 Each Service Order shall be part of this agreement and shall not form a separate contract to it. These terms and conditions for the provision of Services shall apply to any Service Order, including, where support services are provided as stated in the Service Order, those contained in Schedule 1, to the extent of any conflict the following order of priority will apply: (1) any terms expressly agreed on the Service Order; (2) the terms and conditions in the main body of these terms and conditions of Services and (3) the terms and conditions in Schedule 1 to these terms and conditions of Service.

4. DELIVERY OF SERVICES

4.1 The Supplier shall complete the Deliverables and any Milestones for the Services in accordance with the dates specified in an applicable Service Order, or as otherwise agreed in writing between the parties.

4.2 The Supplier shall be given an extension of time for the delivery of any Deliverables and Milestones if one or more of the following events occurs:

4.2.1 agreement in writing between the Supplier and the Customer;

4.2.2 a variation to the Services is made at the Customer's request;

4.2.3 a Force Majeure Event occurs; or

4.2.4 a delay is caused in whole or in part by an action or omission of the Customer or its employees, agents or third-party contractors.

4.3 If the Deliverables and any Milestones are delayed at the request of the Customer, or because of the Customer's or its employees, agents or third-party contractors' acts or omissions, the Service Order shall be amended to take account of such delay. If the Supplier can demonstrate that the delay has resulted in an increase in cost to the Supplier in carrying out its obligations under this agreement, the Supplier may, at its sole discretion, notify the Customer that it wishes to increase the Service Order Charges by an amount not exceeding any such demonstratable cost. The Supplier may invoice the Customer for any additional monies that become payable in this way, within 30 days of demonstrating the increase in costs.

5 SUPPLIER'S RESPONSIBILITIES

5.1 The Supplier shall use its reasonable endeavours to provide the Services from the Services Start Date in accordance with:

5.1.1 Good Industry Practice; and

5.1.2 all Applicable Laws,

in all material respects.

5.2 The Supplier shall:

5.2.1 meet all of its obligations and responsibilities under this agreement;

5.2.2 promptly provide all assistance, information, and advice which the Customer may reasonably require; and

5.2.3 promptly do all acts which the Customer may reasonably request,

to enable the Customer to comply with its obligations under this agreement.

5.3 The Supplier shall use reasonable endeavours to meet any performance dates or Milestones specified in a Service Order but any such dates shall be estimates only and time for performance by the Supplier shall not be of the essence of this agreement. The parties will cooperate in good faith to avoid any delay in the performance of such Milestones and dates and, if such delay arises, the Supplier shall work with the Customer to ensure minimum disruption to the Services.

5.4 The Supplier shall obtain at its own expense the licenses, powers and consents necessary for it to perform its obligations under this agreement.

6. CUSTOMER'S OBLIGATIONS

6.1 The Customer shall:

6.1.1 co-operate with the Supplier in all matters relating to the Services and/or Goods under an applicable Service Order;

6.1.2 meet all its obligations under this agreement;

6.1.3 promptly do all acts which the Supplier may reasonably request;

6.1.4 appoint a manager in respect of each Service Order, who shall have authority to contractually bind the Customer on all matters relating to the Service Order;

6.1.5 provide, for the Supplier, its agents, subcontractors and employees, in a timely manner and at no charge, access to (i) the Customer's premises, equipment, data, assistance, and other facilities as reasonably required by the Supplier and shall ensure that such access is safe and reasonably convenient and (ii) all documents, information, and materials (whether owned by the Customer or a third party) reasonably required by the Supplier and shall ensure that they are accurate and complete in all material respects;

6.1.6 comply with all Applicable Laws as required to enable the Supplier to provide the Services and/or supply the Goods under an applicable Service Order;

6.1.7 obtain and maintain all necessary licenses and consents necessary for the Supplier to provide the Services;

6.1.8 ensure that the Services it is purchasing are suitable for the purposes for which they will be used; and

6.1.9 comply with the Supplier's Acceptable Use policy shown at Annex B of this agreement.

6.2 The Customer warrants to the Supplier that it owns or has the right to use (and grants to the Supplier the right to use) all Customer Materials and Customer's equipment in respect of which the Customer gives access to the Supplier to enable it to provide the Services, and that the Supplier's use of such Customer Materials or Customer's equipment shall not infringe any third party rights or Applicable Laws.

7. SUPPLIER RELIEF

7.1 The Supplier shall not be in breach of this agreement and shall not be liable for any delay in delivery or failure to deliver the part of the Service to which the breach relates or any delay in performance or failure to perform its obligations under this agreement if and to the extent that such delay and/or breach and/or failure is caused by any breach by the Customer of any of its obligations under this agreement.

7.2 If the Supplier incurs additional direct costs in using its reasonable endeavours to perform the Services and/or deliver the Goods under an applicable Service Order as a direct result of any breach by the Customer of its obligations in this agreement it shall be entitled to recover such additional costs from the Customer.

8. CONTRACT MANAGEMENT

8.1 Each party will designate a contract manager who will have day to day responsibility for the performance of their appointer's obligations under this agreement.

8.2 Each party will promptly give the other party details of the person appointed and any changes in that appointment from time to time.

8.3 Each party shall ensure that:

8.3.1 its contract manager is available for consultation by the other party at all reasonable times;

8.3.2 its contract manager and any other relevant personnel attend all meetings reasonably requested by the other party.

8.4 The contract managers shall maintain correspondence by email, by telephone or in person as required and agreed between the parties.

8.5 For the avoidance of doubt, nothing in this clause 8 shall override the Supplier's obligations to provide the Services under this agreement.

9. NON-SOLICITATION

9.1 Customer shall not, without the prior written consent of the Supplier, at any time from the date on which any Services under an applicable Service Order commence to the expiry of six (6) months after the completion of such Services under an applicable Service Order complete, solicit or entice away from the Supplier or employ or attempt to employ any person who is, or has been, engaged as an employee, consultant or subcontractor of the Supplier ("Restricted Person**"**) in the provision of such Services under an applicable Service Order.

9.2 If the Customer commits any breach of this clause 9.1, the Customer shall, on demand, pay to the Supplier a sum equal to one year's basic salary or the annual fee that was payable by the Supplier to the Restricted Person plus the recruitment costs incurred by the Supplier in replacing such person. The parties confirm that these liquidated damages are reasonable and proportionate to protect the legitimate interest of the Supplier.

10. TUPE

The parties acknowledge that it is their understanding that the Transfer of Undertakings (Protection of Employment) Regulations 2006 as amended ("TUPE") do not apply to the commencement of the agreement or any of the Services, or their expiry or termination (however caused). In the event that TUPE does apply under Applicable Laws upon the commencement of the agreement or any of the Services to transfer any persons into the employment of the Supplier, the Customer shall indemnify the Supplier against, pay on demand and make good all liabilities incurred, all damages and loss suffered, all claims demands actions and proceedings made or brought and all costs disbursements and expenses incurred by the Supplier, arising therefrom.

11. CHANGE CONTROL

11.1 Where either party wishes to propose a Change then it will notify the other party of that fact be sending a written request to the other party, specifying in as much detail as is reasonably practicable the nature of the Change.

11.2 The parties shall meet to discuss and agree the scope of the proposed Change including, where applicable, this agreement, any impact on the Services, the practicalities of the Change, the cost of implementation and a timetable for implementation.

11.3 The parties shall use their reasonable endeavours to agree the Change within 20 Business Days of commencing discussions under clause 11.2. Once the Change is agreed, it shall be recorded in writing by the parties (or their authorised representatives).

12 THIRD PARTY SOFTWARE AND DOCUMENTATION

12.1 Where the Supplier provides any Third-Party Software as part of the delivery of the Services, the Supplier shall provide applicable Third Party Software to the Customer under the standard licence terms provided by the relevant third parties, copies of which shall be provided to the Customer where possible and if so requested by the Customer in advance of a Service Order being entered into and the Customer agrees to be bound to the relevant third parties by such licence terms.

12.2 The Supplier shall provide the Customer from time to time with such manuals, including user instruction manuals, operating manuals, technical literature and/or related materials, in human-readable form and on any media, which relate to the use and operation of the Deliverable(s) as is necessary for the proper use of the Deliverable(s) (the "Documentation").

13 CHARGES AND PAYMENT

13.1 The Customer shall pay the Service Order Charges as set out in an applicable Service Order. The Service Order Charges are exclusive of VAT which shall be payable in addition by the Customer to the Supplier at the rate prescribed by law.

13.2 Where the Service Order Charges are calculated on a time and materials basis the Supplier's daily fee rates are calculated on the basis of an eight-hour day, worked during Business Hours.

13.3 The Service Order Charges exclude expenses, which shall be payable by the Customer monthly in arrears as long as such expenses

have been agreed in writing in advance, following submission of an appropriate invoice by the Supplier.

13.4 The Supplier may increase the Service Order Charges in an applicable Service Order on an annual basis (with effect from each anniversary of the Commencement Date) by 3.6%. The first such increase shall take effect on the first anniversary of the Commencement Date.

13.5 The Supplier may, upon no less than one months' notice to the Customer, pass through to the Customer any increases in any input costs or third-party charges arising out of or in connection with the provision of the Goods and/or Services (with accompanying evidence of such increases). If, the cost to the Supplier of providing any Goods increases, the Supplier may before delivery increase the Service Order Charges in respect of the Goods. The Customer acknowledges such increases and agrees to pay such increases in accordance with the agreement.

13.6 As applicable, the Customer shall pay the Supplier for any additional services provided by the Supplier that are requested by the Customer but that are not specified in an applicable Service Order, subject to the instruction for the additional services being given by the contract manager appointed by the Customer in accordance with clause 8.1. Any such charge for additional services shall be invoiced separately from any Service Order Charges due as specified in the Service Order.

13.7 The Supplier shall invoice the Customer for the Service Order Charges at the intervals specified in the Service Order (which may be either in advance or in arrears). If no intervals are so specified in an applicable Service Order, the Supplier shall invoice the Customer monthly in advance.

13.8 The Customer shall pay each invoice submitted to it by the Supplier within 30 days of receipt in full and cleared funds in pounds sterling, by electronic transfer to a bank account nominated in writing by the Supplier from time to time.

13.9 The Customer may dispute in good faith any amounts in an invoice within 30 days of the date of that invoice.

13.10 Without prejudice to any other right or remedy that it may have, if the Customer fails to pay the Supplier any undisputed sum due under this agreement on the due date the Supplier may suspend part or all of the Services or delivery of any Goods under an applicable Service Order until payment has been made in full by the Customer.

13.11. Neither party may withhold payment of any amount due to the other because of any set-off, counterclaim, abatement, or other similar deduction.

14. INTELLECTUAL PROPERTY RIGHTS

14.1 All IPRs belonging to a party prior to the signing of this agreement will remain vested in that party.

14.2 In relation to the Deliverables (excluding the Customer Materials):

14.2.1 the Supplier and its licensors shall retain ownership of all IPRs in the Deliverables.

14.2.2 subject to payment in full of the relevant Service Order Charges, the Supplier grants the Customer, or shall procure the direct grant to the Customer of, a fully paid-up, worldwide, non-exclusive, royalty-free licence to use the Deliverables for the Term of this agreement.

14.3 In relation to the Customer Materials, the Customer:

14.3.1 shall retain ownership of all IPRs in the Customer Materials; and

14.3.2 grants to the Supplier a fully paid-up, worldwide, non-exclusive, royalty-free licence to use, copy and modify the Customer Materials for the term of this agreement for the purpose of providing the Services to the Customer.

14.4 The Customer shall, promptly at the Supplier's request, do (or procure to be done) all such further acts and things and the execution of all such other documents as the Supplier may from time to time require for the purposes of securing for the Supplier all right, title and interest in and to the IPR's assigned to the Supplier in accordance with clause 14.3.2.

14.5 Neither party shall use any IPR's in the other party's trademarks and brands for any purpose without the other party's prior written consent and then only if used in accordance with the other party's instructions as provided from time to time.

14.6 The Customer shall indemnify the Supplier against all damages, losses and expenses arising as a result of any action or claim that the Customer's Materials infringe the IPR's of a third party.

14.7 The Supplier:

14.7.1 warrants that the receipt, use and onward supply of the Services and the Deliverables

by the Customer shall not infringe the rights, including any IPRs, or any third party; and

14.7.2 shall indemnify the Customer in full against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other (reasonable) professional costs and expenses) suffered or incurred by the Customer arising out of, or in connection with, the receipt, use or supply of the Services and the Deliverables.

14.8 The indemnities in this clause 14 are subject to the following conditions:

14.8.1 the indemnified party promptly notifying the indemnifier in writing of the claim.

14.8.2 the indemnified party makes no admissions or settlements without the indemnifier's prior written consent.

14.8.3 the indemnified party gives the indemnifier all information and assistance that the indemnifier may reasonably require; and

14.8.4 the indemnified party allows the indemnifier complete control over the litigation and settlement of any action or claim.

14.9 The indemnities in this clause may not be invoked to the extent that the action or claim arises out of the indemnifier's compliance with any designs, specifications or instructions of the indemnified party.

15. DATA PROTECTION AND DATA PROCESSING

15.1 For the purposes of this clause 15, the following terms shall have the meanings given to them in the Data Protection Legislation: "controller", "processor", "data subject", "personal data", "personal data breach", "process" and "processing"

15.2 Each party collects and processes personal data concerning the other party's employees for the purpose of contract and relationship management in its capacity as a controller and in relation to such personal data that party will comply with its obligations as controller under the Data Protection Legislation.

.

15.2.1 If the Supplier processes any personal data on the Customer's behalf when performing its obligations under this agreement, the parties record their intention that the Customer shall be the data controller and the Supplier shall be a data processor and in any such case shall:

15.2.2 process personal data only on the written instructions of the Customer and the Customer agrees that this agreement shall constitute the Customer's written instructions. If the Supplier is required by any Applicable Laws to process personal data it shall, to the extent legally permitted, notify the Customer before doing so;

15.2.3 have in place appropriate technical and organisational measures to protect against the unauthorised or unlawful processing of Personal Data and against the accidental loss or destruction of, or damage to, Personal Data to ensure a level of security appropriate to (i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage and (ii) the nature of the data to be protected; and

15.2.4 not engage another processor without general written authorisation of the Customer. In order to seek such general authorisation, the Supplier shall provide the Customer with notification of the proposed appointment of the other processor and the Customer shall have 10 Business Days to object to such appointment. If no objection is raised by the Customer, it shall be deemed to have authorised the appointment of the other processor. The Supplier shall ensure that the same data protection obligations as set out in this agreement are imposed on the other processor and the Supplier shall remain fully liable to the Customer for performance of the other processor's obligations to the extent the other processor fails to fulfil their data protection obligations;

15.2.5 ensure that personnel who have access to or process personal data are under contractual or statutory obligations to keep the personal data confidential;

15.2.6 ensure that where personal data is transferred outside of the European Economic Area, such transfer is in accordance with the Customer's instructions and takes place on the following conditions: (i) the transfer is based on adequacy regulations pursuant to Article 45 of UK GDPR and Section 17A of the Data Protection Act 2018; the Supplier participates in a valid cross-border transfer mechanism under the Data Protection Legislation so that the Supplier (and where appropriate the Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required

by Article 46 of UK GDPR; or (iii) the transfer otherwise complies with Data Protection Legislation.

15.2.7 at the Customer's cost, assist the Customer to respond to any request from a data subject;

15.2.8 notify the Customer without undue delay of a personal data breach and, at the Customer's cost, provide reasonable assistance to the Customer complying with its obligations pursuant to Articles 32 to 36 of GDPR;

15.2.9 at the written direction of the Customer, delete or return personal data to the Customer on termination of this agreement unless the Supplier is required by law to store the personal data; and

15.2.10 make available to the Customer all information reasonably necessary to demonstrate compliance with this clause, and, at the Customer's cost, allow for audits conducted by the Customer or its designated auditor. The Customer (or its designated auditor) shall conduct no more than one audit per calendar year except where the Customer believes, acting reasonably and in good faith, that the Supplier may have breached Data Protection Legislation in which case the Customer may conduct additional audits to the extent necessary to determine whether such breach has occurred.

16. CONFIDENTIALITY

16.1 Each party undertakes that it shall not at any time during this agreement, and for a period of three years after termination of this agreement, disclose to any person any Confidential Information concerning the business, affairs, customers, clients or suppliers of the other party, except as permitted by clause 16.2.

16.2 Each party may disclose the other party's Confidential Information:

16.2.1 to its employees, officers, representatives, sub-contractors or advisers who need to know such information for the purposes of exercising the party's rights or carrying out its obligations under or in connection with this agreement. Each party shall ensure that its employees, officers, representatives or advisers to whom it discloses the other party's Confidential Information comply with this clause 16; and

16.2.2 as may be required by Applicable Laws, a court of competent jurisdiction or any governmental or regulatory authority,

provided that, in the case of 16.2.2, the disclosing party shall promptly notify the other party of such requirement (to the extent it is permitted to do so) and such disclosure is on terms that they keep it confidential in compliance with the restrictions set out in this clause 16.

16.3 No party shall use the other party's Confidential Information for any purpose other than to exercise its rights and perform its obligations under or in connection with this agreement.

17. DISPUTE RESOLUTION

17.1 If any dispute between the parties has not been resolved in the normal course of business either party may call a meeting of the parties by service of not less than 10 Business Days' notice and each party agrees to procure that each party's contract manager shall attend a meeting called in accordance with this clause 17.1 with the aim of resolving the dispute.

17.2 Those attending the meeting pursuant to clause 17.1 shall use reasonable endeavours to resolve the dispute(s) arising out of this agreement. If the meeting fails to resolve the dispute within 10 Business Days of it being referred to it, either party by notice in writing may refer the dispute to the Managing Director (or their nominees) of both parties, who shall co-operate in good faith to resolve the dispute as amicably as possible within 15 Business Days of the dispute being referred to them.

17.3 If the dispute between the parties is not resolved having applied the process set out at clause 17.1 and 17.2, then the Dispute Resolution Procedure shall be deemed exhausted and either party may resolve the dispute by any other route, including through the courts.

17.4 Notwithstanding the provisions of this clause 17 either party may commence or take proceedings or seek remedies before the courts of any other competent authority for interim, interlocutory or injunctive remedies in relation to this agreement.

18 LIMITATION OF LIABILITY

18.1 Nothing in this agreement shall limit or exclude the Supplier's liability for:

18.1.1 death or personal injury caused by its negligence;

18.1.2 fraud or fraudulent misrepresentation; or

18.1.3 any other matter that cannot be lawfully excluded.

18.2 Subject to clause 18.1, neither party shall be liable to the other, whether in contract, tort (including negligence), for breach of statutory duty, contract, misrepresentation (whether innocent or negligent), restitution, under indemnity or otherwise, arising under or in connection with this agreement for:

18.2.1 loss of profits (whether direct or indirect);

18.2.2 loss of sales or business (whether direct or indirect);

18.2.3 loss of anticipated savings (whether direct or indirect);

18.2.4 loss of or damage to goodwill;

18.2.5 loss of use or corruption of software, data or information (whether direct or indirect);

18.2.6 or pure economic loss;

18.2.7 (to the extent that the Supplier provides any telecommunications-related Services) telephone call charges originating from or made through the Customer's equipment, whether authorised or unauthorised, and in particular the Supplier is never liable for any expense or charges incurred as a result of toll fraud, phone system hacking or 'phreaking', or dial-through-fraud;

18.2.8 acts or omissions of any other party or (legal or natural) person (other than a sub-contractor of the Supplier) involved with the provision of the Services; and

18.2.9 any indirect, special, or consequential loss, costs, damages, charges or expenses however arising under or in connection with this agreement.

18.3 Subject to clause 18.1 and 18.2, each party's total liability to the other, whether in contract, tort (including negligence), for breach of statutory duty, under indemnity or otherwise, arising under or in connection with this agreement shall be limited to the aggregate value of all Service Order Charges payable by the Customer during the 12 month period immediately preceding the date on which the claim arises or (or, if the claim arises in the first 12 months of the agreement term, the aggregate value of the Service Order Charges due (at the date the claim arises) to be incurred by the Customer in the first 12 months of the agreement term).

18.4 All warranties, representations, conditions and all other terms of any kind whatsoever implied by statute or common law are, to the fullest extent permitted by Applicable Laws, excluded from this agreement.

18.5 To the extent that any Service involves or relies upon internet access, the Supplier does not guarantee uninterrupted internet access.

18.6 Without limitation, the Supplier specifically denies any implied or express representation that the Services and the Deliverables will be fit:

18.6.1 to operate in conjunction with any hardware items or software products other than those that are identified by the Supplier as being compatible with the Deliverables; or

18.6.2 to operate uninterrupted or error-free.

18.7 In all cases (including where a claim is made pursuant to an indemnity), the party making a claim shall mitigate its losses and future losses to the maximum extent reasonably possible.

18.8 The Customer shall indemnify the Supplier and keep the Supplier indemnified against any breach by the Customer of the agreement and any claim brought against the Supplier by a third party resulting from the Customer's breach of its obligations under the agreement or its negligence (including all claims, actions, proceedings, losses, liabilities, costs, expenses, including reasonable legal costs, suffered or incurred by the Supplier) and any liability of the Customer under this clause 18.8 shall be subject to the cap on liability included in clause 18.3.

18.9 For the avoidance of any doubt, references in this clause 18 to the agreement includes any applicable Statements of Work.

19. TERMINATION

19.1 Without affecting any other right or remedy available to it, either party may terminate this agreement with immediate effect by giving written notice to the other party if:

19.1.1 the other party commits a material breach of any term of this agreement and such breach is irremediable or (if such breach is remediable) fails to remedy that breach within a period of 30 days after being notified in writing to do so;

19.1.2 the other party enters into liquidation (other than for the purposes of a bona fide solvent amalgamation or reconstruction) whether compulsory or voluntarily or compounds with its creditors generally or has an administrator, administrative receiver or

receiver appointed over all or a substantial part of its undertaking or assets; or

19.1.3 the other party has become bankrupt or shall be deemed unable to pay its debts by virtue of Section 123 of the Insolvency Act 1986; or

19.1.4 the other party ceases or threatens to cease to carry on business; or

19.1.5 suffers an event which, under the law of a different country, is equivalent to any of the previously specified acts or events; or

19.1.6 a Force Majeure Event continues for a period of 3 months.

19.2 The Supplier may terminate this agreement with immediate effect by giving written notice to the Customer if the Customer fails to pay any amount due under this agreement on the due date for payment and remains in default not less than 14 days after being notified in writing to make such payment, unless a genuine dispute has been notified to the Supplier prior to the due date for payment.

20. CONSEQUENCES OF TERMINATION

20.1 On termination or expiry of this agreement for any reason whatsoever:

20.1.1 the relationship of the parties shall cease and any rights or licenses granted under or pursuant to this agreement shall cease to have effect save as (and to the extent) expressly provided for in this clause 20.1.1

20.1.2 all existing Service Orders entered into before the termination date shall continue until they are terminated or expire in accordance with their own terms;

20.1.3 the Customer shall immediately pay to the Supplier all of the Supplier's outstanding unpaid invoices and interest and, in respect of the Services or Goods supplied but for which no invoice has been submitted, the Supplier may submit an invoice, which shall be payable immediately on receipt;

20.1.4 the Customer shall return all equipment belonging to the Supplier. If the Customer fails to do so, the Supplier may enter the Customer's premises and take possession of such equipment;

20.1.5 each of the parties shall immediately return to the other party (or if the other party so requests by notice in writing, destroy) all of the other party's property in its possession at the date of termination, including all of its Confidential Information, together with all copies of such Confidential Information, and shall make no further use of such Confidential Information; and

20.1.6 any provision which expressly or by implication is intended to come into or remain in force on or after termination shall continue in full force and effect.

20.2 Termination or expiry of this agreement shall be without prejudice to any rights, remedies, obligations or liabilities of either party that may have accrued up to the date of termination or expiry.

21. GENERAL

21.1 The Supplier shall not be liable to the Customer as a result of any delay or failure to perform its obligations under the agreement arising from a Force Majeure Event.

21.2 If the Supplier is delayed or prevented from performing its obligations due to a Force Majeure Event the Supplier shall:

21.2.1 give notice of such delay or prevention to the Customer as soon as reasonably practical stating the commencement date and extent of such delay or prevention, the causes thereof and its estimated duration;

21.2.2 use its reasonable endeavours to mitigate the effects of such delay or prevention upon the performance of its obligations under this agreement; and

21.2.3 resume performance of its obligations as soon as reasonably possible after the removal of the cause of the delay or prevention.

21.3 Neither party shall assign, transfer, mortgage, charge, subcontract, declare a trust over or deal in any other manner with any of its rights and obligations under this agreement without the prior written consent of the other.

21.4 No purported amendment or variation of this agreement or any provision of this agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

21.5 A failure or delay by a party to exercise any right or remedy provided under this agreement or by law shall not constitute a waiver of that or any other right or remedy.

21.6 If any provision or part-provision of this agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted.

21.7 Each party agrees that it shall have no remedy in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this agreement.

21.8 This agreement (and the documents expressly referred to in it, including any extant Service Orders from time to time) constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter. Each party acknowledges and agrees that it has not been induced to enter into this agreement by a statement or promise which it does not contain.

21.9 Each party shall comply with the Bribery Act 2010 and the Modern Slavery Act 2015, and not do, or omit to do any act that will cause the other to be in breach of the Bribery Act or the Modern Slavery Act 2015.

21.10 The parties may communicate with each other in any way that is normal in the course of their business. Any contractual notice given under this agreement shall only be effective if it is in writing, sent to a party at its registered address. Any notice will be deemed to have been duly served if delivered before 4.00 pm on a Business Day, at the time of delivery or, if in any other case at 10.00 am on the next Business Day following the date of delivery; or if posted from within the UK, at 10.00 am on the second Business Day after it was put into the post.

21.11 Nothing in this agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties or constitute any party the agent of another party, and neither party has a right to contract in the name of the other party or make any promises on their behalf.

21.12 This agreement (whether contractual or non-contractual in nature) shall be governed by, and construed in accordance with the law of England and Wales and the parties hereby submit to the exclusive jurisdiction of the courts of England and Wales.

21.13 No party that is not a signatory to this agreement will be entitled to enforce any right or obligation detailed in this agreement, whether under the Agreements (Right of Third Parties) Act 1999 or otherwise

Signature Page

Each party is signing this agreement on the date stated opposite that party's signature. The date of this agreement will be the date stated opposite the signature of the last party to sign it.

SIGNED by a director for and on behalf of
JUNGLE IT LIMITED .....
Director

Print Signatory Name: .....

Print Signatory's Position: .....

Date: .....

SIGNED by a director for and on behalf of
Company Name .....
Director

Print Signatory Name: .....

Print Signatory's Position: .....

Date: .....

SCHEDULE 1

1. DEFINITIONS

The following definitions apply in this Schedule 1:

Remote Monitoring Agent: the software to provide hardware/software inventory, facilitate patching and device remote control.

Service Times: 8.00 am to 6.00 pm on any Business Day. Exclusive of scheduled company training

SLA: the Service Level Agreement, details of which are set out at paragraph 11 of this Schedule 1.

2. MANAGED ENDPOINT

Any variation to the standard Service Times shall be defined in the relevant Service Order. Response times are a goal and not a guarantee. Incidents reported outside Service Times will be deemed to be received at the start of the next Service Time period.

Service desk covers end user devices only. Examples of end user devices include desktop and laptop devices running Microsoft and Apple operating systems as well as mobile devices running Android and Apple operating systems.

Support will cover mainstream operating systems that are in support by the manufacturer as well as common Microsoft end user applications, such as the Office suite, desktop browsers, document readers etc.

The Supplier may require installation of a Remote Monitoring Agent on managed devices to deliver the service. This agent remains the property of the Supplier. It may not be possible to provide the support service if the agent is declined, tampered with or removed. The term 'Remote Monitoring Agent' refers to the software tool deployed by the Supplier to enable monitoring and support of end-user devices.

Incidents may be logged via email, web portal or telephone or any other method provided by the Supplier during the term of the contract. **High priority incidents (P1/P2) must be logged via telephone to ensure the relevant SLA is assigned**. Incidents logged via any other means will initially be classified as P4.

After discussing the incident with the Customer, a mutually agreed priority will be assigned to the incident. The Supplier reserves the right to adjust the priority of the incident as it sees fit throughout the duration of the incident.

All service desk support is remote only. Should the incident not be resolvable remotely, the Supplier will use its reasonable endeavours to provide an engineer on the Customer's site. If the Customer does not subscribe to an on-site support service via a Service Order, then such site visits may be chargeable.

If the incident is as a result of hardware failure, the Supplier will liaise with the relevant hardware manufacturer to provide a repair, provided the Customer has purchased an enhanced warranty for the hardware. For any device that does not have an enhanced warranty, the cost of any repair/replacement will be the responsibility of the Customer and the SLA's will not apply.

The Supplier shall deploy Microsoft's Monthly Security Update Release (MSUR) via Supplier's Remote Monitoring and Management (RMM) agent. The Microsoft MSUR contains security updates and quality updates, tool updates and minor feature updates. End-user devices must have the Supplier's RMM agent installed to enable the deployment of the MSUR. The Supplier maintains an internal MSUR validation process, including a test plan managed by the Network Operations Centre (NOC) which assesses the release and determines whether they should be accepted or withheld based on stability and security considerations. This process is designed to reduce risk but does not guarantee compatibility with the Customer's specific environment.

End-user devices occasionally require a hard restart to invoke the MSUR. The supplier shall force this restart should it be required. Applications not included within the MSUR (i.e. Third-Party Security Updates - TPSU's) are updated separate Third-Party restricted to the applications available within the RMM platform. The Customer is responsible for testing all MSUR's and TPSU's and releases within their environment to ensure compatibility and co-existence with their applications and infrastructure and must notify the Supplier in advance if any MSUR or TPSU should be withheld from deployment.

Upon request the Supplier may configure test groups for the Customer that deploy all available MSUR's and TPSU's via RMM. TPSU's are restricted to the availability of the update via the RMM platform and may not cover all applications within the Customers environment. A list of all currently available Applications is available upon request. MSUR's and TPSU's may contain bug-fixes and feature updates within the update package. The Supplier shall not be held liable for any issues, disruptions, or damages

resulting from the application of the MSUR or any TPSU, whether standard or extended.

Any patching outside the scope of the above, including operating system updates, feature updates, or bespoke patching requests, must be explicitly requested by the Customer and may be subject to additional charges.

The service desk support service will **not** include the following unless specified separately in the Service Order:

- resolution of incidents due to errors in customer software, including viruses or malware introduced by the Customer or the Customer's agents;
- resolution of incidents due to the installation or upgrading of software or hardware by the Customer or the Customer's agents;
- resolution of incidents due to the Customer or the Customer's agents moving, changing, removing or otherwise making any changes without prior notification and acceptance by the Supplier;
- training of end users on the use of hardware and software;
- providing advice on how to use software features;
- any other issue not considered 'break-fix';
- software/hardware that is no longer supported by the manufacturer; or
- unlicensed software.

The Supplier may maintain documentation and an asset record of hardware, software and additional services as required to provide the support service. This documentation remains the property of the Supplier and will not be shared without a documentation release fee being payable by the Customer to the Supplier, the sum of which shall be notified to the Customer by the Supplier if required.

Upon termination of the service, the Supplier may charge offboarding fees to support the transition to a new provider. These fees will be communicated in advance and must be settled before the offboarding process is completed.. The Supplier will continue to charge the Customer for any software or service consumed after the termination of service. The Supplier shall be entitled to submit an invoice to the Customer for all outstanding payments in relation to such offboarding charges. Such invoice must be satisfied in full before the Supplier can complete the offboarding process for the Customer.

Support is charged per device. The Supplier's Remote Monitoring Agent will automatically detect new devices that are connected to the Customer network and charges will be adjusted appropriately. It is the Customer's responsibility to notify the Supplier if a device is to be retired to prevent unnecessary charges being made. A device may be removed automatically if it has not reported to the Supplier's systems for a period of 3 months. Device count is variable but will not be reduced below the initial number of devices during the term of the Service Order.

3. MANAGED SECURITY OPERATIONS CENTRE

The Managed Security Operations Centre (SOC) service is included as part of the Managed Endpoint Service, where explicitly stated on a service order. It provides continuous monitoring and response to security threats across supported endpoint devices and Microsoft 365 environments, as specified in the applicable Service Order.

This includes:

- real-time threat detection using Microsoft Defender, and SIEM tools,
- automated and manual containment actions,
- escalation to Jungle IT analysts for communication to customer within contracted hours; and/or
- monitoring of identity and device activity.

The Managed SOC Service does **not** include:

- forensic investigation beyond initial triage,
- legal or regulatory reporting, and
- remediation of third-party systems not under the Supplier's management

Limitation of Liability for Managed SOC Service

- The Managed SOC Service provides monitoring and response for security threats. While the Supplier will take reasonable steps to detect and contain threats, no security solution can guarantee complete prevention.
- In addition to the limits of liability in the terms and conditions (in particular, clause 18) the Supplier is not liable to the Customer whether in contract, tort (including negligence), for breach of statutory duty, contract, misrepresentation (whether innocent or negligent), restitution, under indemnity or otherwise, arising under or in connection with this agreement for any data

loss, business interruption, or damages resulting from a security breach.

The Customer is responsible for:

- ensuring all managed devices have the Supplier remote monitoring agent installed and operational
- ensuring that the relevant Microsoft and Defender licensing is provisioned and configured to support monitoring and reporting
- maintaining up-to-date user access controls and Multi Factor Authentication (MFA) policies and conditional access policies, and
- informing the Supplier of any changes to its environment that may affect monitoring and/or the provision of Managed SOC Services.

4. MANAGED SECURITY

The managed security service provides management and monitoring of the Customer's IT security. Managed security is broken down into four separate security offerings.

Client Anti-Virus Management

The Supplier's Anti-Virus Management service is included as part of the Managed Endpoint agreement. All devices with the Supplier's agent installed will be actively monitored for compliance with the Managed Anti-Virus solution.

Apple devices will be manually configured during the initial service setup to ensure proper integration with the Anti-Virus management platform.

In consultation with the Customer, the Supplier will configure and install policies to control periodic and on-access scanning arrangements.

The Supplier will check the status of individual devices to ensure anti-virus definitions are up to date and that the anti-virus software is present and functioning. Where devices are part of the Managed Endpoint service, the Supplier will investigate and remediate issues relating to out-of-date definitions or missing anti-virus software.

Devices not covered under ta Managed Endpoint agreement and that have not reported in for more than 30 days will be highlighted to the Customer, via a monthly report, who retains sole responsibility to investigate and remediate. The Supplier shall not be liable in any way whatsoever for any losses incurred as a result of the Customer failing to investigate and remediate any non-reporting devices where the Supplier has reported to the Customer of such.

Where detected, security outbreaks will be contained by the Supplier if the device is covered under the Managed Security Operations Centre (SOC) service. The incident will be reported to the Customer for remediation, or the Supplier can resolve the issue for an additional charge.

Unless explicitly stated in the Service Order, the Supplier will not provide support for incidents caused by security outbreaks outside the scope of the Managed SOC service.

Firewall Management

The Supplier will provide an enterprise-grade firewall solution as part of the Managed Firewall Service. This includes configuration changes, ongoing management, and regular updates to ensure optimal performance and security.
Customers are entitled to up to five configuration changes per calendar month at no additional cost. Requests exceeding this limit may incur additional charges, which will be communicated in advance.

The Supplier will support one firewall rule audit per calendar year, upon request by the Customer. This audit will be conducted in collaboration with the Customer to review the relevance and effectiveness of existing firewall rules.

As part of this process, the Supplier will assist in identifying and removing any rules deemed redundant or outdated. Additional audits or rule reviews outside the annual entitlement may be subject to additional charges.

Service charges apply per firewall device, with a minimum contract term of 36 months.

To enable enhanced reporting features, the Managed Firewall Service collects and processes internet activity data on Jungle's secure servers. This data may include information classified as sensitive personal data. By subscribing to this service, the Customer consents to this processing. Customers who wish to opt out of data processing must notify the Supplier in writing.

FortiAnalyzer

By accessing and using FortiAnalyzer, customers agree to the terms governing its implementation within their organisation's security infrastructure.

FortiAnalyzer operates as a centralised platform that consolidates telemetry across networks, endpoints, and cloud environments. It utilises a unified data lake, built-in automation, native threat intelligence, and AI-driven assistance to enhance detection and response capabilities.

Customers acknowledge that FortiAnalyzer ingests, normalises, and enriches data from various sources within the Fortinet Security Fabric, providing structured dashboards and actionable insights to support informed decision-making. Integration with FortiGuard Labs delivers continuous threat intelligence, automated outbreak detection, and risk-based scoring aligned with the MITRE ATT&CK framework.

By using FortiAnalyzer, the client acknowledges and accepts that the service collects and processes network data, including but not limited to websites visited, traffic patterns, and user activity logs, to enhance threat investigation, accelerate incident identification, and improve overall security posture. All data processed through FortiAnalyzer must comply with applicable data protection legislation and internal organisational policies.

Email Filtering

The email filtering service includes the provisioning and configuration of a mail filtering (Spam Protection) system.

The Supplier will fully manage the system including 10 changes per month. Additional changes may be subject to a charge. Changes include white/blacklisting, release of quarantined items etc.

Charging is variable, based on number of mailboxes detected.

Web Filtering

The web filtering service includes the provisioning and configuration of a web filtering system.

The Supplier will fully manage the system including 10 changes per month. Additional changes may be subject to a charge.

Charging is variable, based on number of users detected.

5. MANAGED BUSINESS CONTINUITY

Managed Backup

This service requires Jungle IT's backup agent installed on each device.

The Managed Backup service provides secure, off-site cloud backups using dedicated Datacentre infrastructure and industry-leading software. The service utilises industry leading and agent-based software to automate backup, de-duplicate and store data efficiently and securely off-site. Managed Backup is a managed cloud backup service using Datacentre facilities and equipment specified for backups. The service utilises industry leading and agent-based software to automate backup, de-duplicate and store data efficiently and securely off-site.

The Managed Backup service provides secure, off-site cloud backups using dedicated Datacentre infrastructure and industry-leading software. The service utilises industry leading and agent-based software to automate backup, de-duplicate and store data efficiently and securely off-site.

In consultation with the Customer, the Supplier will configure and install agents to backup physical and/or virtual servers and/or Microsoft 365 and/or workstations. Backups will run on a scheduled basis as per the agreed Recovery Point Objectives with the customer at onboarding

The Customer is responsible for agreeing the backup sets with the Supplier to ensure all required data is backed up successfully. The Supplier will accept no responsibility for any data that is not recoverable from the managed backup service. Where necessary, the Customer is responsible for the safe keeping of any encryption keys to allow successful restoration of data from backup sets.

Any additional servers and/or workstations must be notified by the Customer for inclusion in the backup schedule. Office 365 users and included automatically and will increase the backup user count incurring additional charges.

The Customer is responsible for informing the Supplier of any servers, users, mailboxes or workstations which are no longer needed to be backed up. Deletion of a user account in Office 365 does not automatically delete the backup data and costs will still be incurred. The Supplier will not remove backup data unless specifically requested to do so.

The Supplier will monitor backup status daily, investigate failures, and take remediation actions where possible and monthly backup health reports will be provided to the Customer.

Backups will be encrypted in transit and at rest using industry-standard encryption. If there are issues relating to the server, workstation or 365 tenant outside of the backup agent itself, this will be passed back to the customer to resolve and then a manual backup can be requested.

Full restores (Bare Bones) are available for servers, but out of scope for workstations due to the unique nature of the workstation expected to be enrolled in this service

Managed Service will **not** include the following unless specified separately in the Service Order:

- resolution of incidents due to errors in customer software, including viruses or malware introduced by the Customer or the Customer's agents;
- resolution of incidents due to the installation or upgrading of software or hardware by the Customer or the Customer's agents;
- resolution of incidents due to the Customer or the Customer's agents moving, changing, removing or otherwise making any changes without prior notification and acceptance by the Supplier;
- any other issue not considered 'break-fix';
- software/hardware that is no longer supported by the manufacturer; or
- unlicensed software.

Upon termination of the service, the Supplier may charge offboarding fees to support the transition to a new provider. These fees will be communicated in advance and must be settled before the offboarding process is completed.

Managed Azure DR

Managed ASR is a managed cloud replication service using Microsoft's Azure platform. The service utilises agent-based software to replicate, failover and recover data efficiently and secure off-site.

In consultation with the Customer, the Supplier will configure and install agents to replicate physical and/or virtual servers on a periodic basis.

The Supplier will be proactively alerted to any failures when they occur ensuring successful investigation and completion. Any failures will be investigated, and remediation action put in place, where possible. Alerts relating to server process or service failures will be passed back to the customer to resolve unless covered by our Managed Server service. The Customer will receive a monthly report detailing proactive alerts received by the Supplier.

The supplier will only act on alerts that are correctly reported to our service management platform and are not responsible for any alerts that are not received and alerts will only be actioned during our normal working service hours - 8am to 6pm unless covered by our 24x7 support offering.

Additional data on already configured devices will be automatically replicated but may incur extra charges due to the offsite storage size increasing. Any additional servers added will be the Customer's responsibility to inform the Supplier to ensure it is added to the replication schedule.

The Customer is responsible for agreeing the replication policies with the Supplier to ensure all required servers are replicated successfully. The Supplier will accept no responsibility for any data that is not recoverable from the Managed Azure DR service.

Additional Azure costs incurred during Tests are not included in the above costs and will be passed to the client as part of their monthly Azure Consumption invoice.

Invocation and failback costs are not covered through the monthly service and will be charged at a minimum of three days at our standard day rate of £950. With any extra time taken charged in addition to the minimum three days stated.

The Supplier will provide support for Managed Azure Disaster Recovery (DR) services as part of the Customer's broader Business Continuity and Disaster Recovery (BCDR) strategy. Invocation of the DR process will be governed by a customer owned playbook, created in collaboration between the Customer and the Supplier. The Supplier's role is limited to assisting with and executing the steps

outlined in this playbook. The overall ownership, maintenance, and governance of the BCDR plan including invocation, decision-making authority and responsibility for its completeness and effectiveness remains solely with the Customer. The Supplier will not be liable for any outcomes resulting from the invocation of the BCDR plan beyond the scope of the agreed playbook.

6. MANAGED SERVER

Any variation to the Service Times shall be defined in the Service Order. Response times are a goal and not a guarantee. Incidents reported outside Service Times will be deemed to be received at the start of the next Service period.

Managed Server covers physical server and virtual server devices only. Devices must be running Microsoft or Enterprise versions of Linux operating system.

The Supplier may require installation of a Remote Monitoring Agent on managed devices to deliver the service. This agent remains the property of the Supplier. It may not be possible to provide the support service if the agent is declined, tampered with or removed. The term 'Remote Monitoring Agent' refers to the software tool deployed by the Supplier to enable monitoring and support of end-user devices

Incidents may be logged via email, web portal or telephone or any other method provided by the Supplier during the term of the contract. **High priority incidents (P1/P2) must be logged via telephone to ensure the relevant SLA is assigned.** Incidents logged via any other means will initially be classified as a P4.

After discussing the incident with the Customer, a mutually agreed priority will be assigned to the incident. The Supplier reserves the right to adjust the priority of the incident as it sees fit throughout the duration of the incident.

All Service Desk support is provided remotely . Where an incident cannot be resolved remotely, the Supplier may, at its sole discretion, offer to dispatch an engineer to the Customer's site. Such on-site attendance may incur additional charges, which will be communicated in advance where reasonably practicable.

If the incident is as a result of hardware failure, the Supplier will liaise with the relevant hardware manufacturer to provide a repair, provided the Customer has purchased an applicable warranty for the hardware. For any server that does not have an enhanced warranty, the cost of any repair/replacement will be the responsibility of the Customer and the SLAs will not apply.

The Supplier shall deploy Microsoft's Monthly Security Update Release (MSUR) via Supplier's Remote Monitoring and Management (RMM) agent. The Microsoft MSUR contains security updates and quality updates, tool updates and minor feature updates. End-user devices must have the Supplier's RMM agent installed to enable the deployment of the MSUR. The Supplier maintains an internal MSUR validation process, including a test plan managed by the Network Operations Centre (NOC) which assesses the release and determines whether they should be accepted or withheld based on stability and security considerations. This process is designed to reduce risk but does not guarantee compatibility with the Customer's specific environment.

End-user devices occasionally require a hard restart to invoke the MSUR. The supplier shall force this restart should it be required. Applications not included within the MSUR (i.e. Third-Party Security Updates - TPSU's) are updated separate Third-Party restricted to the applications available within the RMM platform. The Customer is responsible for testing all MSUR's and TPSU's and releases within their environment to ensure compatibility and co-existence with their applications and infrastructure and must notify the Supplier in advance if any MSUR or TPSU should be withheld from deployment.

Upon request the Supplier may configure test groups for the Customer that deploy all available MSUR's and TPSU's via RMM. TPSU's are restricted to the availability of the update via the RMM platform and may not cover all applications within the Customers environment. A list of all currently available Applications is available upon request. MSUR's and TPSU's may contain bug-fixes and feature updates within the update package. The Supplier shall not be held liable for any issues, disruptions, or damages resulting from the application of the MSUR or any TPSU, whether standard or extended.

Any patching outside the scope of the above, including operating system updates, feature updates, or bespoke patching requests, must be explicitly requested by the Customer and may be subject to additional charges.

Managed Service will **not** include the following unless specified separately in the Service Order:

- the Service Desk Support Service shall not include: resolution of incidents arising from errors in Customer-owned software,

including but not limited to viruses or malware introduced by the Customer or its agents.

- resolution of incidents due to the Customer or the Customer's agents moving, changing, removing or otherwise making any changes without prior notification and acceptance by the Supplier;
- training of users on the use of hardware and software;
- providing advice on how to use software features;
- any other issue not considered 'break-fix';
- software/hardware that is no longer supported by the manufacturer; or
- unlicensed software.

The Supplier may maintain documentation and an asset record of hardware, software and additional services as required to provide the support service. This documentation remains the property of the Supplier and will not be shared without a documentation release fee being payable by the Customer to the Supplier, the sum of which shall be notified to the Customer by the Supplier if required.

Upon termination of the service, the Supplier may charge offboarding fees to support the transition to a new provider. These fees will be communicated in advance and must be settled before the offboarding process is completed.

The Supplier will continue to charge the Customer for any software or service consumed after the termination of service. The Supplier shall be entitled to submit an invoice to the Customer for all outstanding payments in relation to such offboarding charges. Such invoice must be satisfied in full before the Supplier can complete the offboarding process for the Customer.

Support is charged per server. The Supplier's Remote Monitoring Agent will be installed on servers procured and built by the Supplier and charges will be adjusted appropriately. It is the Customer's responsibility to inform the Supplier when a server is procured or built outside of the Supplier's standard procurement process. This ensures that appropriate support can be provided. Servers that do not have the Supplier's monitoring agent installed are not covered under the support agreement. It is the Customer's responsibility to notify the Supplier if a server is to be retired to prevent unnecessary charges being made. Server count is variable but will not be reduced below the initial number of servers during the term of the Service Order.

7. MANAGED INFRASTRUCTURE

Any variation to the standard Service Times shall be defined in the Service Order for the service taken. Response times are a goal and not a guarantee. Incidents reported outside Service Times will be deemed to be received at the start of the next Service Time period.

Managed Infrastructure covers Customer's Enterprise Grade Infrastructure devices only.
Devices not provided by the Supplier must have a manufacturer support agreement in place that mirrors the support offered by the Supplier. All devices must be in mainstream support by the manufacturer. Devices without suitable manufacturer support may be supported on a best-endeavours basis.

Incidents may be logged via email, web portal or telephone or any other method provided by the Supplier during the term of the contract. High priority incidents (P1/P2) **must** be logged via telephone to ensure the relevant SLA is assigned. Incidents logged via any other means will initially be classified as a P4.

After discussing the incident with the Customer, a mutually agreed priority will be assigned to the incident. The Supplier reserves the right to adjust the priority of the incident as it sees fit throughout the duration of the incident.

All Managed Infrastructure support is remote only. Should the incident not be resolvable remotely, the Supplier will use its reasonable endeavours to provide an engineer on the Customer's site. If the Customer does not subscribe to an on-site support service via a Service Order, then such site visits may be chargeable.

If the incident is as a result of hardware failure, the Supplier will liaise with the hardware manufacturer to provide a repair, provided the Customer has purchased an extended warranty for the hardware. For any device that does not have an extended warranty, the cost of any repair/replacement will be the responsibility of the Customer and the SLA's will not apply.

Incidents will be classified as P4 if hardware cover is not in place.

Managed Service will **not** include the following unless specified separately in the Service Order:

- resolution of incidents due to errors in customer software, introduced by the Customer or the Customer's agents;

- resolution of incidents due to the installation or upgrading of software or hardware by the Customer or the Customer's agents.
- resolution of incidents due to the Customer or the Customer's agents moving, changing, removing, or otherwise making any changes without prior notification and acceptance by the Supplier.
- any other issue not considered 'break-fix'.
- software/hardware that is no longer supported by the manufacturer.
- unlicensed software; or
- periodic patching of firmware or system software.

Upon termination of the service, the Supplier may charge offboarding fees to support the transition to a new provider. These fees will be communicated in advance and must be settled before the offboarding process is completed. Support is charged per physical and virtual device. The Supplier's Remote Monitoring Agent will automatically detect new devices and charges will be adjusted appropriately. It is the Customer's responsibility to notify the Supplier if a device is to be retired to prevent unnecessary charges being made. Device count is variable but will not be reduced below the initial number of devices during the term of the Service Order.

8. MANAGED MICROSOFT

Microsoft 365

The Supplier will provide first line support and fault diagnosis with escalation to the distributor partner for second and third line support and fix.

Managed Azure

Any variation to the Service Times shall be defined in the Service Order. Response times are a goal and not a guarantee. Incidents reported outside Service Times will be deemed to be received at the start of the next Service period.

Our Managed Azure service incorporates our Managed Server service for any virtual machines within the Azure estate. Please refer to this section of our Terms of Service for further detail.

Services out of Scope include:

- Applications monitoring and management
- License management for windows, RDS Cals
- Implementation of cloud optimization recommendations
- Resource provisioning or services setup

The Supplier may require installation of an Enterprise App in the Customers Azure tenancy and Remote Monitoring Agent on managed devices to deliver the service. The agent and App remains the property of the Supplier. It may not be possible to provide the support service if the agent and/or app is declined, tampered with or removed

Incidents may be logged via email, web portal or telephone or any other method provided by the Supplier during the term of the contract. High priority incidents (P1/P2) must be logged via telephone to ensure the relevant SLA is assigned. Incidents logged via any other means will initially be classified as a P4.

After discussing the incident with the Customer, a mutually agreed priority will be assigned to the incident. The Supplier reserves the right to adjust the priority of the incident as it sees fit throughout the duration of the incident.

Managed Service will **not** include the following unless specified separately in the Service Order:

- resolution of incidents due to errors in customer software, including viruses or malware introduced by the Customer or the Customer's agents;
- resolution of incidents due to the installation or upgrading of software or Azure services by the Customer or the Customer's agents;
- resolution of incidents due to the Customer or the Customer's agents moving, changing, removing or otherwise making any changes without prior notification and acceptance by the Supplier;
- any other issue not considered 'break-fix';
- software or Azure services that are Beta or no longer supported by the manufacturer; or
- unlicensed software.

Support is charged as a percentage of Azure consumption incorporating virtual devices, Infrastructure as a service (Iaas) resources, Platform as a service (PaaS) resources and non-compute. It is the Customer's responsibility to inform the Supplier when an Azure subscription is added, or a server is built outside of the Supplier's standard process. This ensures that appropriate support can be provided. Azure Subscription and Servers that do not have the Supplier's monitoring agent installed are not covered under the support agreement. It is the Customer's responsibility to notify the Supplier if an Azure subscription or server is to be removed/retired to prevent unnecessary charges being made. Server count is variable but will not be reduced below the initial number of servers during the term of the Service Order. Upon termination of the service, the

Supplier may charge offboarding fees to support the transition to a new provider. These fees will be communicated in advance and must be settled before the offboarding process is completed.

9. MANAGED CONNECTIVITY

The Supplier will provide first line support and fault diagnosis with escalation to communications provider for second and third line support and fix. Different types of connectivity carry different support levels and response times and will be detailed in carrier terms and conditions.

The Supplier provides support for connectivity and routers supplied under this agreement. Support for other devices is excluded. Communication lines supplied by the Supplier provide first line fault diagnosis with second and third line support provided by the communications Provider.

The Customer is responsible for connectivity and communication provided by other means or providers.

10.MANAGED VOICE

The Supplier's managed voice service includes provision of cloud-based telephone (soft phone or hardware) and support, including basic add/moves/changes. The Supplier will fully manage the system including 10 changes per month. Additional changes may be subject to a charge.

Hardware supplied by the Supplier is covered under the manufacturer's warranty on a return-to-base basis.

Applications used to make calls are supported by the relevant carrier. The Customer is responsible for the devices on which these applications are installed, unless those devices are already covered under the Supplier's Managed Endpoint Service.

Firmware and application updates are provided by the respective manufacturers or network providers.

11. MANAGED END USER COMPUTE

Device Lifecycle Management

The Supplier will provide an end-to-end device logistics services. The exact nature of the service depends on the service taken and will be described on the service order. The following services can be requested:

- Liaise with company HR team for new user/movers/leavers
- Unbox, removing and recycling all unnecessary packaging. Perform device inspection for any defects
- DOA check and notification for remediation. Supplier to manage - Distributors with DOA issues, if procured by Supplier
- Asset Tag Device.
- Image of Device Via Autopilot and Intune.
- Provision device as per user profile, ensuring correct domain membership and application deployment
- Repackage ready for storage.
- Stock Reporting of Assets as determined.
- Delivery to office or end user home address
- Collection of devices from leavers.
- Cleaning and restocking of returned devices.
- Secure disposal of end-of-life devices,
- Dealing with warranty repairs if under manufacturer's warranty.

Additional bespoke features such as personalized instructions, accessories and company merchandising can all be included and specified within the service order. Engineering work is undertaken at our Technical Operations Centre where hardware is stored securely for delivery to end users, either in the office or at their home address.

Managed Intune

Any variation to the standard Service Times shall be defined in the Service Order for the service taken. Response times are a goal and not a guarantee.

Incidents reported outside Service Times will be deemed to be received at the start of the next Service Time period.

Incidents may be logged via email, web portal or telephone or any other method provided by the Supplier during the term of the contract. High priority incidents (P1/P2) must be logged via telephone to ensure the relevant SLA is assigned. Incidents logged via any other means will initially be classified as a P4

After discussing the incident with the Customer, a mutually agreed priority will be assigned to the incident. The Supplier reserves the right to adjust priority of the incident as it sees fit throughout the duration of the incident. Managed Intune is a remote only reactive support agreement that covers the Customer's Intune environment.

Managed Intune will not include the following unless specified separately in the Service Order:

- creating packages to push out new applications
- resolution of incidents due to the installation or upgrading of software or hardware by the Customer or the Customer's agents;
- resolution of incidents due to the Customer or the Customer's agents moving, changing, removing or otherwise making any changes without prior notification and acceptance by the Supplier;
- any other issue not considered 'break-fix';
- software/hardware that is no longer supported by the manufacturer; or
- unlicensed software

12. SERVICE LEVEL AGREEMENT

Priority	Response Time	Escalation Level 1	Escalation Level 2	Escalation level 3	Communication Level
P1	15 Mins	Immediate	Immediate	Immediate	Hourly
P2	1 Hour	2 Hours	4 Hours	2 days	Every 4 hours
P3	4 Hours	8 Hours	1 day	Never	Daily
P4	8 Hours	2 Days	Never	Never	Monthly
P5	16 Hours	5 Days	Never	Never	Monthly

Key To Priority	Affecting Multiple People	Affecting Single Person
High (site, service or main LOB application unavailable)	P1	P2
Medium (system is unacceptably slow or degraded)	P2	P3
Low (system is slow and/or tasks more difficult than usual)	P3	P4
Request Fulfilment (minor adds, moves, changes)	P5	P5

Escalation Level 1	2nd/3rd Line Engineer
Escalation Level 2	Manager
Escalation Level 3	Director

13. SERVICE ESCALATION

Should the Customer feel it needs to escalate a request for any reason, the below table will assist the Customer in this process.

The Customer should quote the unique ticket ID whenever it escalates an incident or request.

Escalations are available during contracted support hours only. A charge may be made for escalations made outside of contracted Service Times.

Level	Contact	Position
1	Findlay.wightman@jungleit.co.uk	Head of IT Operations – 07519326904
2		
3	richard.knight@jungleit.co.uk	Operations Director - 07970742400

SCHEDULE 2 – SERVICE ORDER

Delivery Location			
"Company Name & Address"			
Resold Services			
1.			
2.			
3.			
4.			
Services	**Quantity**	**Unit Price per month**	**Total per month**
5.			
6.			
7.			
8.			
Total Monthly		£ 0	

Additional Terms
This Service Order is subject to the Terms and Conditions for the Provision of IT Services entered into between the parties on the Commencement Date.

ANNEX A

CONTRACT RECONCILIATION SCHEDULE

Reconciliation is defined as the difference between the amount invoiced in advance for a specific period against the actual delivered/consumed amount for services for the same period.

The reconciliation will occur in the first week of each month for the previous month. Any adjustments will be included in the following months invoice.

Invoice Month	Contract Services Period Reconciled
January	December
February	January
March	February
April	March
May	April
June	May
July	June
August	July
September	August
October	September
November	October
December	November

ANNEX B

Acceptable Use Policy

This Acceptable Use Policy (AUP) is intended to help protect the Supplier's clients, and the Internet community, from the inappropriate use of the Internet. A Customer's use of the Supplier's Services constitutes acceptance of this AUP. The Supplier reserves the right to revise and update this AUP from time to time. The Supplier expects Customers to cooperate with the Supplier's TOS/Abuse department when requested to assist in their investigations.

1. **General Violations**

1.1. Our AUP prohibits the following:

Impersonation/Forgery

1.1.1. Adding, removing, or modifying identifying network header information ('spoofing') in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited (the use of anonymous re-mailers and nicknames does not constitute impersonation). Using deliberately misleading headers ('munging' headers) in news postings in order to avoid spam e-mail address collectors is allowed provided appropriate contact information is contained in the body of the posting. Privacy violations attempts, whether successful or unsuccessful, to gain access to any electronic systems, netservices or data, without proper consent, are prohibited. Threats of bodily harm or destruction of property are prohibited. Threatening or harassing activity is prohibited. The use of any Supplier Service for illegal purposes is prohibited. The resale of any Supplier Service without proper authorisation from the Supplier is prohibited.

Network Disruptions and Network-Unfriendly Activity

1.1.2. Any activities, which adversely affect the ability of other people or systems to use Supplier Services or the Internet, are prohibited. This includes 'denial of service' (DoS) attacks against another network host or individual user.

1.1.3. Interference with, or disruption of, use of the network by others, network services or network equipment is prohibited.

1.2. It is the Customer's responsibility to ensure that their network is configured in a secure manner. A Customer may not, through action or inaction, allow others to use their network for illegal or inappropriate actions. A Customer may not permit their network, through action or inaction, to be configured in such a way that it gives a third party the capability to use their network in an illegal or inappropriate manner.

2. E-Mail

2.1. The Supplier does not tolerate, endorse or participate in e-mail spamming. Sending unsolicited commercial e-mail is prohibited. The Supplier cannot authorise bulk e-mailing although the Supplier does recognise that in some instances this is a valid and useful form of marketing for both senders and recipients.

2.2. Using an e-mail or Web site address supplied by Supplier to collect responses from unsolicited commercial e-mail is prohibited.

2.3. Sending large volumes of unsolicited e-mail, whether or not that e-mail is commercial in nature is prohibited. All solicited e-mail should have been confirmed through the use of a double opt-in list (i.e. the recipient must confirm their wish to receive that particular e-mail twice).

2.4. Activities that have the effect of facilitating unsolicited commercial e-mail, or large volumes of unsolicited e-mail, whether or not that e-mail is commercial in nature, are prohibited. Users operating mail servers must ensure that they are not open relays.

2.5. Anonymous bulk e-mailings are not permitted and the Supplier will terminate the accounts of any Customers who attempt to do this. This may happen without notice.

2.6. If the Supplier receives any complaints from recipients or other third parties, or any mailing causes technical problems on our systems, the Supplier may take further action to stop this happening again. This may involve the termination of any accounts the sender has and may occur without notice.

2.7. The Customer shall comply in full with all obligations upon the Customer under the Data Protection Act 2018.

3. Facilitating a Violation of this AUP

Advertising, transmitting, or otherwise making available any software, programme, product, or service that is designed to violate this AUP, or the AUP of any other Internet Service Supplier, which includes, but is not limited to, the facilitation of the means to spam, is prohibited.

4. Newsgroups

4.1. Customers should use their best judgment when posting to any newsgroup. Many groups have charters, published guidelines, FAQs, or 'community standards' describing what is and is not considered appropriate. Usenet can be a valuable resource if used properly. The continued posting of off-topic articles is prohibited. Commercial advertisements are off-topic in most newsgroups, especially non-commercial regional groups. The presence of such articles in a group is not indicative of the group's intended use. The Customer must familiarise themselves with basic USENET netiquette before posting to a newsgroup.

4.2. Newsgroup spamming: Spam is, first and foremost, a numerical metric-posting of substantively similar articles to multiple newsgroups. This form of spam is sometimes referred to as 'excessive multi-posting' (EMP). The Supplier considers 'multi-posting' to 10 or more groups within a two-week period to be excessive.

4.3. Hostile attacks or invectives (flames) aimed at a group or individual posters are generally considered inappropriate in Supplier service groups. Many newsreaders offer filtering capabilities that will bring certain messages to the Customer's attention or skip over them altogether (kill files).

4.4. Customers may not cancel messages other than their own messages. A Customer may cancel posts forged in that Customer's name. The Supplier may cancel any postings that violate this AUP.

5. Web

5.1. Using a Web site address or hosted Web account supplied by Supplier for the purpose of distributing illegal material is prohibited.

5.2. Using a Web site address or hosted Web account supplied by Supplier to collect responses from unsolicited commercial e-mail is also prohibited.

6. Excessive Bandwidth or Disk Utilisation

6.1. Supplier account descriptions specify current limits on bandwidth and disk utilisation. Where limits are not specifically defined the judgement of the Supplier Internet Technical Support team shall be used to define those limits. The use of bandwidth or disk space in excess of those limits is not permitted. The total number of bytes transferred from an account's Web and FTP space determines bandwidth utilisation. The total number of bytes required to store an account's Web, FTP, and Mail data determines disk utilisation.

6.2. If the Supplier determines that excessive bandwidth or disk space utilisation is adversely affecting the Supplier's ability to provide Services (to any of the Supplier's customers), the Supplier may take immediate action which may (in the Supplier's discretion) include suspension of availability of the Customer's Services over the internet (or the availability of the Internet itself). The Supplier will attempt to notify the account owner by e-mail as soon as possible.

7. Reporting to the Supplier's TOS/Abuse Department

7.1. The Supplier requests that anyone who believes that there is a violation of this AUP should direct the information to the Supplier's AUP Abuse Staff.

7.2. Customers who wish to report 'spam' from a non-Supplier source should send copies of the e-mail they received along with full header information. Some messages may not receive a response, but the Supplier may use the information received to aid in the development of the Supplier's filter lists.

7.3. All issues involving other e-mail abuse originating from Supplier e-mail or network addresses should also be sent to the Supplier.

7.4. All material published must be owned by the publisher or the appropriate releases must have been obtained prior to publishing.

7.5. The Supplier may (without limiting its other rights or remedies) take any one or more of the following actions in response to complaints:

7.5.1. Issue warnings: written or verbal

7.5.2. Suspend the Customer's newsgroup posting privileges

7.5.3. Suspend the Customer's account

7.5.4. Terminate the Customer's account

7.5.5. Invoice the Customer for administrative costs and/or reactivation charges

What information should be submitted?

1. The IP address used to commit the alleged violation

2. The date and time of the alleged violation, including the time zone or offset from GMT

3. Evidence of the alleged violation

Copies of e-mail with full header information provide all the required information, as do syslog files and firewall logs. Other situations will require different methods.