



Master Service Agreement

Our address
Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

Give us a call
[0333 939 8080](tel:03339398080)

Send us a message
hello@jumpsec.com

Find out more
www.jumpsec.com

MASTER AGREEMENT FOR CYBER SECURITY SERVICES

(Including Managed Detection & Response (MDR), Continuous Attack Surface Management (CASM) and cyber security consultancy)

This Agreement (the "Agreement") is made and entered into as of **[Effective Date]** (the "Effective Date"), by and between:

The Parties

JUMPSEC Ltd, a company incorporated and registered in England and Wales with company number 08327063, whose registered office is at Unit 3E-3F, 33-34 Westpoint, Warple Way, Acton, W3 0RG ("JUMPSEC" or the "Supplier"); and

[Client Name], a company incorporated and registered in **[Jurisdiction]** in England and Wales with company number **[Client Company Number]**, whose registered office is at **[Client Address]** ("Client").

Background

- (A) ☐ JUMPSEC is a provider of cybersecurity services, including but not limited to Managed Detection & Response (MDR), Continuous Attack Surface Management (CASM) and consultancy, which are designed to protect organisations from evolving cyber threats.
- (B) ☐ The Client wishes to engage JUMPSEC to provide these security services in accordance with the terms and conditions set forth in this Agreement and any associated Service Specific Schedules, Statements of Work, or Appendices.
- (C) ☐ This Agreement sets out the legal framework under which JUMPSEC will provide services to the Client, including terms relating to service delivery, data processing, service levels, and contractual obligations.

Interpretation & Structure

This Agreement is comprised of the following documents, which together form the entire agreement between the Parties:

- i. This Master Agreement (including its Terms and Conditions).
- ii. The Service Specific Schedule applicable to the services being provided.
- iii. Any applicable Statements of Work (SoW), Proposals, or commercial terms documents.
- iv. The Data Processing Agreement (DPA) (where applicable, in compliance with UK GDPR/EU GDPR).

- v. The Service Level Agreement (SLA) defining the service commitments and performance standards.

In the event of a conflict between the documents:

- i. The Statement of Work (SoW) or Proposal shall take precedence over the Master Agreement.
- ii. The Service Specific Schedule shall take precedence over general terms in the Master Agreement.
- iii. The DPA and SLA shall govern their respective subject matters but shall not override other fundamental contractual terms unless expressly stated.

1. Definitions and Interpretations

- 1.1 Unless inconsistent with the context, the words and expressions below will have the following meanings and similar expressions will have the same meanings:

"Affiliate" means any entity that controls, is controlled by, or is under common control with a Party;

"Agreement" this document including the Service Specific Schedule or appendices annexed to this document and the Proposal;

"Business Day" means any day other than a Saturday, Sunday, bank or public holiday in the country that the contracting JUMPSEC entity is situated in;

"Business Hours" mean the hours between 09:00 and 17:00 on Business Days;

"Confidential Information" in relation to either Party or its Affiliates, is information that:

- i. is by its nature confidential; and/or
- ii. is designated by that Party as confidential; and/or
- iii. the other Party knows or ought to know is confidential; and/or
- iv. including but not limited to deliverables, trade secrets, know-how, inventions, techniques, processes, software, documentation, procedures, contracts, customer information, financial information, ideas, strategies, designs, projections, business plans, strategic expansion plans, unpublished information relating to the Intellectual Property of either Party and all communications between the Parties.

"Customer Portal" means the relevant online portal to facilitate communication between the Parties including the secure transfer of files or documents;

"Data Controller" shall have the same meaning as outlined in the DPA;

Deleted: ¶

“Data Protection Legislation” means as applicable (i) the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (Directive on privacy and electronic communications) (as amended), Commission decisions and guidance and all national implementing legislation; (ii) Gramm–Leach–Bliley Act provisions relating to Non-public Personal Information, (iii) the UK Data Protection Act, 2018 (iv) the South African Protection of Personal Information Act, 2013 (v) all other applicable laws and regulations relating to data protection and privacy in any jurisdiction in which the Personal Data is being processed;

“Data Subject” shall have the same meaning as outlined in the DPA;

“DPA” means the Data Processing Appendix attached to this Agreement;

“Effective Date” means the date on which this Agreement is signed by both Parties, or the date specified as the commencement date in the applicable Statement of Work (SoW) or Service Specific Schedule, whichever is earlier.

“Intellectual Property” will be interpreted widely and will mean the patents; trade names, marks and secrets; designs; know-how; copyright; goodwill; and such other registered or unregistered patents, trademarks, trade names, rights of copyright, symbols, signs, insignia, emblems, logos, slogans, and items relating to JUMPSEC or the Services and all other identical or similar Intellectual Property as may exist anywhere in the world which is not in the public domain and any applications for registration of such Intellectual Property;

“Personal Data” shall have the same meaning as outlined in the DPA;

“Proposal” shall have the same meaning as “Statement of Work”;

“Services” will mean any of the Services and/or Deliverables provided by JUMPSEC under this Agreement;

“Service Date” means the agreed date specified in the Proposal as the date on which the Services will commence;

“Service Fees” means the amount payable to JUMPSEC by the Client as consideration for the Services, as outlined in the Proposal;

“Service Specific Schedule” means the unique terms that are specific to a Service within a schedule to this agreement;

“Statement of Work” means the formal documents agreed in writing by the Parties containing the offer and scope of Services and the Service Fees;

“Time And Materials” means a pricing model under which the Client agrees to pay JUMPSEC based on the actual time spent performing the Services at the agreed rates and the cost of materials, expenses, or third-party products required for delivery, as specified in the Statement of Work.

1.2 Interpretations

- 1.2.1 Any reference in this Agreement to an enactment is to that enactment as at the date of signature hereof and as amended or re-enacted from time to time;
- 1.2.2 A reference to a Party includes that Party's successors-in-title, Affiliates and permitted assigns;
- 1.2.3 Any one gender includes the other genders; the singular includes the plural and vice versa;
- 1.2.4 The Proposal will take precedence in the event of any conflict between the Proposal and this agreement.

2. Duration and Application

- 2.1 This Agreement will apply to the Services and will be effective from the date that both Parties sign this Agreement and will continue in full force and effect until **terminated in accordance with Clause 11.1.**
- 2.2 Any specific terms applicable to the Services not covered herein, will be integrated as a Service Specific Schedule.

3. General JUMPSEC obligations

- 3.1 In addition to the specific obligations of JUMPSEC set out in the Proposal and in this Agreement, JUMPSEC will:
 - 3.1.1 ensure the necessary security clearance is performed for each employee who is involved with the Services;
 - 3.1.2 use reasonable endeavours to meet any performance dates specified in the Proposal;
 - 3.1.3 deliver the Services to the Client with reasonable care, quality and skill in a manner consistent with the provisions of this Agreement;
 - 3.1.4 ensure that its employees devote such time, attention and skill in performing the Services as may be reasonably required for the proper discharge of its duties under this Agreement;
 - 3.1.5 have and maintain appropriate insurance in effect for the duration of this Agreement to cover any reasonable and foreseeable claims that may arise while rendering the Services;

- 3.1.6 provide the Services in accordance with good practices and in conformance with codes and standards established for such Services, but gives no warranties in respect of the Services, except for any warranties which may be specifically agreed in writing between JUMPSEC and the Client;
- 3.1.7 provide the Client with access to all relevant information, co-operation and assistance relating to the Services as the Client may reasonably require.

4. General Client obligations

- 4.1 In addition to the specific obligations of the Client set out in the Proposal and in this agreement, the Client will:
 - 4.1.1 provide to JUMPSEC, or procure for JUMPSEC, such cooperation, support and advice, information and documentation as are reasonably necessary to enable JUMPSEC to provide the Services;
 - 4.1.2 ensure that all governmental, legal or regulatory licenses and permits as reasonably required from the Client are obtained prior to the commencement of the Services;
 - 4.1.3 ensure that any affected employees or other Data Subjects of the Client have given their consent for Personal Data to be processed as relevant and required before the commencement of the Services;
 - 4.1.4 inform JUMPSEC, as soon as reasonably practical, when any Client employees with access to any Customer Portal, leave the employment of the Client;
 - 4.1.5 afford JUMPSEC and its personnel with access to the Client's premises and other facilities as reasonably required to deliver the Services;
 - 4.1.6 be responsible to restore any aspects of the Client's hardware, firmware and software that required a change before the Services could commence to the state that it was before or to an improved state, where applicable.

5. Anti-bribery and corruption

- 5.1 The Parties undertake to:
 - 5.1.1 fully comply with all applicable anti-bribery and corruption laws and relevant policies;
 - 5.1.2 not do or omit to do, any act that will cause a breach of applicable anti-bribery and corruption laws.

6. Non-solicitation

- 6.1 The Client agrees that, for a period of 24 months following the termination of this Agreement, it shall not, directly or indirectly:

6.1.1 Solicit for employment, hire, or engage any JUMPSEC employee who was involved in delivering the Services.

6.1.2 Use a third-party recruiter or contractor to circumvent this restriction.

6.2 In the event of a breach, the Client shall pay JUMPSEC liquidated damages equal to 100% of the employee's annual salary as compensation for recruitment and training costs..

7. Confidentiality

7.1 Confidential Information disclosed by one Party to the other, will only be disclosed and/or used as is strictly necessary for the purpose for which it was disclosed and in accordance with the provisions of this Agreement.

7.2 Each Party warrants and undertakes that it will not at any time disclose to any person or entity any Confidential Information of the other Party except as permitted by clause 7.1.

7.3 The confidentiality obligations will not apply to Confidential Information which was:

7.3.1 at the time of disclosure generally available to the public other than because of a breach of this Agreement;

7.3.2 at the time of such disclosure was already within the possession of the receiving Party;

7.3.3 subsequently provided to the receiving Party by a person who has not directly or indirectly obtained the Confidential Information from the disclosing Party and/or through a breach of this Agreement;

7.3.4 received from a third party who lawfully acquired the Confidential Information;

7.3.5 generally disclosed by the disclosing Party to others on an unrestricted basis;

7.3.6 reproduced or disclosed under due legal process.

7.4 The receiving Party undertakes to the disclosing Party:

7.4.1 to ensure that its employees, officers, representatives or advisers to whom it discloses the other Party's Confidential Information are aware and strictly comply with the provisions of this Agreement;

7.4.2 to take reasonable steps to safeguard the Confidential Information and comply with any reasonable requirements specified by the disclosing Party from time to time;

7.4.3 to implement rigorous security practices against any unauthorised copying, use, disclosure, access, damage, dissemination or destruction of the Confidential Information or part thereof, whether directly or indirectly by any other person, or

to assist any other person in doing so, without the prior written consent of the disclosing Party, first being obtained;

7.4.4 to immediately notify the disclosing Party if the receiving Party suspects or becomes aware of any unauthorised access, copying, use or disclosure of the Confidential Information in any form or if the receiving Party is required by law to disclose any of the Confidential Information;

7.4.5 to, in the event of an unauthorised disclosure or use of the Confidential Information through a disclosure made to a receiving Party, use all reasonable efforts to assist the disclosing Party in recovering and preventing the use, dissemination, sale or other disposal of such Confidential Information.

7.5 The Parties acknowledge that they are entitled to equitable relief (in addition to any other rights available under this Agreement or at law) if any Party breaches any of its obligations under this clause 7.

8. Invoicing and payment

8.1 In consideration of the provision of Services by JUMPSEC, the Client will pay the Service Fees as outlined in the Proposal.

8.2 The Client will pay all invoices within fourteen (14) days following receipt of a correct, valid and original invoice together with the required supporting documentation.

8.3 Service Fees are exclusive of value added tax ("VAT") as relevant, which will be payable, in addition to such amounts, at the rate applicable on the date of invoicing.

8.4 All amounts due under the Agreement will be paid in full without any set-off, counterclaim, deduction or withholding.

8.5 Service Fees exclude any surcharges, levies, sales, use, excise, withholding or similar taxes whatsoever unless otherwise agreed in the Proposal.

8.6 Should withholding taxes be applicable, whereby the Client is legally compelled to withhold such taxes, then the Parties will agree on the invoicing and payment thereof, so that JUMPSEC may receive the total net amount payable for the Services.

8.7 The Client will pay the Service Fee into JUMPSEC's bank account as it appears on the relevant invoice and JUMPSEC will formally communicate any change in bank detail to the Client.

8.8 Where the Service Fees are calculated on a time and materials basis:

8.8.1 JUMPSEC's standard day rates for each individual person are calculated based on an eight-hour day, worked during Business Hours;

8.8.2 JUMPSEC will be entitled to charge an overtime rate of 150% of the standard day rates for any time worked outside Business Hours on a Business Day; and

8.8.3 JUMPSEC will be entitled to charge an overtime rate of 200% of the standard day rate for any time worked on a day that is not a Business Day.

8.9 Without affecting any other right or remedy available to it, JUMPSEC may suspend the Services and reserves the right to charge interest on the outstanding balance of all amounts due and payable but unpaid by the Client at the rate of 4% above the base rate from time to time of the Bank of England.

9. Postponements and cancellations

9.1 The Client may postpone any Service Date, if such postponement is agreed to in writing and done in accordance with the relevant Service Specific Schedule.

9.2 JUMPSEC reserves the right to charge for any late postponements or cancellations by the Client. If applicable, the terms will be covered in the relevant Service Specific Schedule and/or Proposal.

10. Travel policy

10.1 The Client will be responsible for all local and international travel and subsistence expenses incurred by JUMPSEC employees when delivering the Services.

10.2 All travel requirements will be confirmed by JUMPSEC at the commencement of the Services for approval by the Client.

10.3 The Client requirements in respect of location and/or standard rates will be considered by JUMPSEC, but JUMPSEC will retain the right to make travel arrangements at its own discretion.

10.4 Where accommodation cost is higher due to security requirements (i.e. security escorts, security complex etc.), the Client will be informed of any such additional cost prior to the commencement of the Services.

11. Data protection

11.1 The Parties will comply with all applicable requirements of any relevant Data Protection Legislation.

11.2 If relevant to the Service, the Parties will enter into a data processing agreement, which shall contain details of any data processing activities.

11.3 Without prejudice to the generality of section 11.1, the Parties will, in relation to any Personal Data processed in connection with the performance of its obligations under this Agreement:

11.3.1 process that Personal Data only on the written instructions of the Data Controller unless otherwise required by applicable laws;

- 11.3.2 ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss, damage or destruction thereof and that such measures are appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the Personal Data to be protected;
- 11.3.3 have regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data) ensuring confidentiality, integrity, availability and resilience of its systems;
- 11.3.4 further ensure that availability of and access to Personal Data can be restored in a timely manner after an incident by regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it;
- 11.3.5 ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential;
- 11.3.6 not transfer any Personal Data outside of the European Economic Area or other applicable area unless the following conditions are fulfilled:
 - 11.3.6.1 the Data Subject has enforceable rights and effective legal remedies;
 - 11.3.6.2 the Parties comply with their obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred;
 - 11.3.6.3 the Parties comply with reasonable instructions notified to it in advance by the Data Controller with respect to the processing of the Personal Data;
- 11.3.7 assist the Data Controller in responding to a reasonable request from a Data Subject without undue delay;
- 11.3.8 notify the Data Controller without undue delay on becoming aware of a Personal Data breach;
- 11.3.9 at the written direction of the Data Controller, delete or return Personal Data and copies thereof to the Data Controller on termination of the Services or this Agreement, unless required by applicable law to store the Personal Data; and
- 11.3.10 maintain complete and accurate records and information to demonstrate its compliance with this clause 11.

12. Breach and termination

- 12.1 Should a Party ("the Defaulting Party") commit a breach of any of the provisions of this Agreement, then the other Party ("the Aggrieved Party") will be entitled to require the Defaulting Party to remedy the breach within 10 (ten) Business Days, or any other reasonable time, of delivery of a written notice requiring it to do so.
- 12.2 If the Defaulting Party fails to remedy the breach within the period specified in such notice, the Aggrieved Party will be entitled to claim immediate performance by the Defaulting Party of all the Defaulting Party's obligations whether the due date for such performance will have arrived, in either event, without prejudice to the Aggrieved Party's right to claim damages.
- 12.3 The provisions of clause 12.2 are without prejudice to such other rights as the Aggrieved Party may have at law.
- 12.4 Early Termination Fees:

12.4.1. If the Client terminates the Agreement before the end of the agreed Subscription Period, the Client shall:

- i. Pay JUMPSEC a termination fee equal to 50% of the remaining contract value, payable within 30 days of termination.
- ii. Reimburse JUMPSEC for all incurred but unrecovered costs, including third-party software licensing and personnel costs.

12.4.2. If the Client terminates within 30 days of the contract start date, the Client shall remain liable for the full first-year contract value.

- 12.5 The right to terminate this Agreement in terms of this section will not prejudice any other right or remedy of either Party in respect of any prior breach of this Agreement.
- 12.6 Any other or specific provisions regarding the termination of the Services may be addressed in the Proposal and/or Service Specific Schedule.

13. Consequences of termination

- 13.1 All invoices issued by JUMPSEC will become due and payable immediately following the termination of this Agreement for whatever reason.
- 13.2 The Confidentiality (clause 7), Data Protection (clause 11), Intellectual Property (clause 16) and Alternative Dispute Resolution (clause 17) provisions and obligations herein will survive the termination of this Agreement.
- 13.3 Any termination of this Agreement will be without prejudice to any claim which a Party may have in respect of any prior breach of the terms of this Agreement by the other Party.

13.4 This Agreement will continue to apply in full until all such fixed terms have elapsed.

14. Limitation of liability

14.1 Nothing in this Agreement limits any liability which cannot be legally limited, including liability for:

14.1.1 death or personal injury caused by negligence;

14.1.2 fraud or fraudulent misrepresentation; and

14.1.3 **if relevant, breach of the terms implied by clause 2 of the UK Supply of Goods and Services Act 1982.**

14.2 For all events and circumstances, JUMPSEC's total aggregate liability for any claims arising under or in connection with this Agreement shall be limited to the lesser of:

- i. 100% of the total Service Fees paid in the 12 months preceding the claim, or
- ii. £250,000

14.3 JUMPSEC shall not be liable for:

- i. Any indirect, incidental, or consequential damages, including but not limited to loss of business, loss of profits, reputational harm, or loss of anticipated savings.
- ii. Any loss of data or security breach that results from (i) the Client's failure to implement JUMPSEC's recommended remediations, (ii) pre-existing security vulnerabilities, or (iii) Client-side misconfigurations.
- iii. Any third-party claim unless caused by JUMPSEC's wilful misconduct.
- iv. **Force Majeure events, as defined in Clause 15.**

14.4 This clause is severable from the rest of the Agreement and will remain in effect even if the Agreement is terminated.

15. Force majeure

15.1 Neither Party will be deemed in default of this Agreement, nor will it hold the other Party responsible for interruption or delay in the performance of its obligations (excluding payment obligations) for circumstances which rise that were not foreseeable or avoidable with reasonable care ("Force Majeure Event") provided that the Party relying on **this clause 15 gives** prompt written notice of the cause, nature and extent of the Force Majeure Event and takes all steps reasonably necessary to limit the effects thereof.

15.2 If the circumstances change after the affected Party has notified the other Party in accordance with clause 15.1, the affected Party will, forthwith, in good faith and by the

most expeditious means, inform the other Party of such changes and keep the other Party updated on such changes.

- 15.3 Any Services affected by a Force Majeure Event will be rescheduled at the termination of the Force Majeure Event to the first available timeslot in the JUMPSEC delivery schedule.
- 15.4 If a Force Majeure Event extends for a period exceeding 30 (thirty) days in total, either Party may elect to terminate this Agreement upon written notice.

16. Intellectual property

- 16.1 All Intellectual Property that belong to or is licensed to a Party will remain vested in that Party.
- 16.2 The Parties record and the Client acknowledges that all right, title and interest in and to all Intellectual Property, including without limitation, copyright, of any materials used by JUMPSEC relating to the Services is and will remain the property of JUMPSEC, both during the term of this Agreement and after termination of this Agreement.
- 16.3 The property and any copyright or other Intellectual Property rights in any material produced by JUMPSEC will belong to JUMPSEC, but the Client will be entitled to use it for the purposes of utilising the Services by way of a non-exclusive license, subject to payment in full of all Service Fees payable under this Agreement.
- 16.4 The Client will not sub-license, assign or otherwise transfer the rights granted in clause 16.3 unless agreed in writing by JUMPSEC.
- 16.5 JUMPSEC warrants that any material produced by JUMPSEC for use by the Client for the purposes of utilising the Services will not infringe on the Intellectual Property rights or other rights of any third party.
- 16.6 The Client warrants that the material and access provided to JUMPSEC for purposes of providing the Services will not infringe on any Intellectual Property rights or other rights of any third parties.

17. Alternative dispute resolution

- 17.1 In the event of a dispute between the Parties of any kind or nature relating to this Agreement, upon the written request of either Party, each Party will appoint a senior representative whose task it will be to meet to resolve such dispute. Such representatives will discuss and negotiate the matter in dispute in good faith, as to resolve the dispute on mutually agreeable terms
- 17.2 In the event of failing to reach amicable settlement, the CREST Complaints and Resolutions Measures, as detailed in the CREST Code of Conduct, shall be applied. Should the dispute remain unresolved following the CREST Complaints and

Resolutions Measures the dispute will be submitted to and decided through mediation, failing by means of arbitration through CEDR or any other mutually agreed upon institution.

- 17.3 For purposes making an arbitration award an order of court, each Party hereby submits itself to the jurisdiction of any court having jurisdiction over the party against whom the award is made.
- 17.4 Both Parties will continue to comply with all the provisions of this Agreement with all due diligence during the determination of such dispute, should the dispute arise during this Agreement.
- 17.5 This clause 17 is severable from the rest of this Agreement and will remain in effect, even if this Agreement is terminated for any reason.

18. Notices

- 18.1 Any notice given to a Party under or in connection with this Agreement will be in English, in writing and delivered (i) personally or (ii) by a recognised courier service to a Party's chosen address or (iii) sent by email by an authorised official or (iv) with prepaid (return receipt requested) first-class or registered post.
- 18.2 Any notice to a Party will be deemed received:
 - 18.2.1 on the date of delivery if contained in a correctly addressed envelope and delivered and signed for by a responsible person during ordinary business hours at its chosen address; or
 - 18.2.2 on the first Business Day following its deposit with the courier service for next Business day delivery; or
 - 18.2.3 when the sender of the email has received an automated message confirming email delivery; or
 - 18.2.4 on the day the receiving Party signature is obtained when sent by prepaid first-class or registered post.

19. General

- 19.1 Entire Agreement - This Agreement contains the entire agreement between the Parties in relation to the subject matter.
- 19.2 Variation - No amendment or variation to this Agreement will be of any force or effect unless it is in writing and signed by the duly authorised representatives of both Parties.
- 19.3 No waiver - The failure of either 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.

- 19.4 Cession, assignment and other dealings - Neither Party to this Agreement may cede, assign, transfer, mortgage, charge, declare a trust over, subcontract or delegate all or any portion of its rights, obligations nor liabilities under this Agreement without the prior consent of the other Party, which consent may not unreasonably be withheld, provided that either Party will be entitled to assign, cede or delegate any of its rights or obligations to an Affiliate.
- 19.5 Severability - If any clause, section or provision of this Agreement should be invalid, unenforceable, defective or illegal for any reason whatsoever, then the remaining terms and provisions of this Agreement will be deemed to be severable from such clause or section and will continue in full force and effect unless such invalidity, unenforceability, defect or illegality goes to the root of this Agreement.
- 19.6 Costs - Each Party will bear its own costs and expenses relating to the negotiation, preparation and execution of this Agreement.
- 19.7 Relationship - JUMPSEC will serve as an independent contractor or service provider, and under no circumstances will it be, or be deemed to be, a partner, joint venture or employee of the Client in the performance of its duties and responsibilities pursuant to this Agreement. All employees engaged by JUMPSEC will be JUMPSEC's employees and the entire management, direction, and control of all such employees will be exclusively vested with JUMPSEC.
- 19.8 Good faith - The Parties undertake to act in the utmost good faith in their relationship with each other and they undertake not to do anything nor refrain from doing anything which might prejudice or detract from the rights or interests of the other Party.
- 19.9 Export control – in the event of any subsequent re-export, the Client must comply with any applicable export control laws.
- 19.10 Counterpart - This Agreement may be signed in counterparts and the copies signed in counterpart will form this Agreement. This will include scanned copies of this document.

20. Governing law and jurisdiction

- 20.1 All the provisions of this Agreement will be governed by and interpreted in accordance with the laws of England and Wales.
- 20.2 The Parties agree to the non-exclusive jurisdiction of the courts of England and Wales.

In witness, this AGREEMENT has been duly executed.

	JUMPSEC	Client
--	----------------	---------------



Authorised Signatory		
Position / Title		
Date of Signature		
Signature		
Company Name		
Company Registration Number		
Company Address		

SERVICE SPECIFIC SCHEDULE – JUMPSEC Managed Services

This Service Specific Schedule for JUMPSEC Managed Services is entered into on the date that both Parties have signed this agreement and will be subject to the terms of the Agreement. The definitions used but not defined in this Service Specific Schedule shall have the meanings given in the agreement.

1. Specific terms for the service

1.1 Definitions

“Agent” means Software deployed by JUMPSEC’s which enables the delivery of the Service;

“Cloud Service” means a service made available to users on demand via the Internet;

“Client-site Equipment” any equipment located on the Client’s premises but controlled by JUMPSEC as part of the Service, as outlined in section 4;

“Customer Portal” the interface by which the Client can access service related information;

“Effective Date” is as defined in the Agreement;

“Go Live Date” the date the Service commences;

“Service Level Agreement” defines the levels of the Service provided as outlined in the Proposal;

“Subscription Period” means the agreed duration for which the Service will be delivered to the Client by JUMPSEC.

2. Term and termination

- 2.1 The Agreement will commence on the Effective Date and continue for the initial period shall continue in full force and effect until terminated in accordance with Clause 3.
- 2.2 Renewal of services shall be subject to mutual agreement and confirmation in writing at least three (3) months prior to the expiry of the existing term.
- 2.3 The Parties may agree in writing, no later than three (3) months before the end of the current Subscription Period, to terminate the Services. In the event of such termination, the final thirty (30) days of the Subscription Period shall be spent uninstalling the Service and the Service Level Agreement shall not apply for such period.

- 2.4 Any Services required after the expiry of the Subscription Period without termination thereof or the renewal of such Subscription Period will be subject to the standard JUMPSEC emergency day rates.
- 2.5 In the event that the Go Live Date is delayed through fault or negligence of the Client, JUMPSEC:
- 2.5.1 will not be held liable for the delivery of the Service or the adherence to the Service Level Agreement during the period of the delay; or
- 2.5.2 reserves the right to keep to the agreed Go Live Date despite the provisions of section 3.2.
- 2.6 The duration of specific services will be governed by the Service Specific Schedule and Statement of Work (SoW) applicable to each service engagement.

3. Term and termination

Deleted: ¶

- 2.1 The Subscription Period will commence on the Go Live Date and continue for the initial period as outlined in the Agreement. Any subsequent Subscription Periods will, unless otherwise agreed in writing by the Parties, be of the same duration as the first Subscription Period but no less than twelve (12) months.
- 2.2 Following the initial Subscription Period, the Parties shall meet in good faith to discuss the renewal of the Subscription Period at least three (3) months prior to the lapse of the current Subscription Period.
- 2.3 The Parties may agree in writing, no later than three (3) months before the end of the current Subscription Period, to terminate the Services. In the event of such termination, the final thirty (30) days of the Subscription Period shall be spent uninstalling the Service and the Service Level Agreement shall not apply for such period.
- 2.4 Any Services required after the expiry of the Subscription Period without termination thereof or the renewal of such Subscription Period will be subject to the standard JUMPSEC emergency day rates.
- 2.5 In the event that the Go Live Date is delayed through fault or negligence of the Client, JUMPSEC:
- 2.5.1 will not be held liable for the delivery of the Service or the adherence to the Service Level Agreement during the period of the delay; or
- 2.5.2 reserves the right to keep to the agreed Go Live Date despite the provisions of section 3.2.

4. Supply of Services

- 3.1 JUMPSEC will provide the Services in accordance with the Service Level Agreement.

- 3.2 If the Client wishes to postpone the Go Live Date, JUMPSEC will attempt to accommodate such a request. Should the Client not agree to a new commencement date within three (3) months of the original Go Live Date, then the Client will, irrespective of Services being performed or not, remain liable for payment of all Service Fees due for the first twelve (12) months of the Subscription Period, which will become due and payable in-full within thirty (30) days of the date of invoice.
- 3.3 Following the completion of the Services it will be the responsibility of the Client to perform uninstallation of software and reconfigure firewalls and other aspects of the Client's hardware, firmware and software, which were included for the performance by JUMPSEC of the Services. JUMPSEC will, upon request, provide all information reasonably required for this purpose.
- 3.4 Where JUMPSEC identifies a potential or actual threat, all reasonable attempts will be made to notify the Client (in accordance with the agreed communication procedure). JUMPSEC will not be liable where it is not possible to contact authorised nominees outside of agreed timescales for reasons outside of JUMPSEC's control.
- 3.5 JUMPSEC shall notify the Client in writing of any upgrades in the Services.

5. Cloud Services

- 4.1 Parts of the Service may be delivered using a Cloud Service.
- 4.2 The Client undertakes to provide JUMPSEC full and unfettered access to any resource related to the Cloud Service as and when required so that JUMPSEC can communicate between Service components internal to the Client network and the Cloud Service.

6. Changes of scope

- 5.1 A material change in the scope of the Services may result in an amendment to the Service Fees as defined in the Proposal. Material changes may include, but are not limited to, the addition of new networks for monitoring or an increase in endpoints.

7. Customer Portal

- 6.1 JUMPSEC will provide the Client with a Customer Portal in accordance with the Service Level Agreement.
- 6.2 The purpose of the Customer Portal is to provide a platform for the Client and JUMPSEC to interact for any matters relating to the Services.
- 6.3 The Client can access the Management Information on the Customer Portal, the content of which will be agreed between the parties and deployed within a reasonable timeframe.

- 6.4 Security event and incident management and reporting will be via separate secure communications channels in accordance with the Service Level Agreement and in accordance with the agreed communication procedure.

8. Service Fees and Charges

- 7.1 The Service Fees are as outlined in the Proposal.
- 7.2 JUMPSEC will invoice the Client in accordance with the invoicing schedule set out in the Proposal.
- 7.3 JUMPSEC will invoice the Client for subsequent years of the Subscription Period on the anniversary of the Go Live Date unless otherwise agreed.
- 7.4 All prices will remain valid for a period of thirty (30) days following the Proposal date, and shall be subject to confirmation thereafter. All changes to project scope must be agreed in writing by both Parties.
- 7.5 All Service Fees may be adjusted on an annual basis, effective on each anniversary of the Go Live Date, to reflect any increases in the CPI of the previous twelve (12) months.
- 7.6 If the implementation of the Services is delivered in one phase, an invoice may be issued on acceptance of the Proposal. The Client agrees to provide a purchase order within ten (10) Business Days of acceptance of the Proposal.
- 7.7 All reasonable expenses incurred by JUMPSEC in the delivery and/or implementation of the Services will be charged by JUMPSEC to the Client. The Client agrees to issue a purchase order within ten (10) Business Days of the date that JUMPSEC makes a valid request.
- 7.8 If any purchase order is not issued or any invoice is not paid by the due date, JUMPSEC reserves the right, in addition to its other remedies, to not proceed and/or suspend the Services and any related support. The rights to suspend the Services are not exhaustive.

Appendix A - Software License

Description and Minimum Requirements

The Service provided by JUMPSEC may rely on Software Agents deployed on the Client's network. JUMPSEC may, with agreement of the Client, amend which Software Agents are deployed with the sole goal to protect against likely or live cyber threats and attacks. The Software will be deployed across the Client's IT estate and can be remotely managed by JUMPSEC.

This Agreement does not include any Software procured and deployed by the Client which may be used by JUMPSEC to provide the Service.

1. Definitions

- 1.1 Definitions capitalised but not defined shall have the meanings given in the Agreement and/or Service Specific Schedule.

"Authorised Users" mean those users who are authorised by the Client to use the Software;

"Custom Detection" means the documented rulesets developed specifically for the Client.

"Documentation" the documents relating to the Software provided by JUMPSEC to the Client, including the deployment guide;

"Maintenance Services" the performance of scheduled and/or preventative maintenance services required to ensure the continued functionality of the Software, including the provision and installation of upgrades, updates, enhancements and new releases;

"Software" the agents or components LimaCharlie and Velociraptor or and any other security services software required by JUMPSEC for use in the Service;

"Client" means any person using or procuring the Software.

2. Grant of Software License and Acceptance by User

- 2.1 In the provision of the Services, JUMPSEC may make use of certain Software, which will be deployed by the Client using their own deployment mechanisms.
- 2.2 JUMPSEC hereby grants to the Client, a non-exclusive and non-transferrable license to use the Software in accordance with the terms herein for the duration of the Service Specific Schedule.
- 2.3 The license to use the Software and any other related rights are subject to the continued use of the underlying Service procured by the Client from JUMPSEC and will terminate immediately upon the Service being terminated by either Party.

3. Delivery and Installation

- 3.1 Where Software is required the Client will receive Software for the Agents from JUMPSEC via secure means.
- 3.2 Where required, the Client warrants that their network complies with the minimum system requirements for installation of the Software, as outlined in the installation and product guides provided by JUMPSEC.
- 3.3 JUMPSEC shall notify the Client in the event of a change to the minimum system requirements.
- 3.4 JUMPSEC and the Client may, at the request of the Client, enter into a written agreement in terms of which the Client is given a degree of control over which capabilities are installed via the Agents, as well as the time of installation of such capabilities.
- 3.5 Where the Parties have not entered into a separate written agreement allowing the Client to have control over the specific capabilities and time of installation via the Agent, all capabilities will be installed by JUMPSEC, at the discretion of JUMPSEC, via the Agent, with or without the prior knowledge of the User. In any event, JUMPSEC would use all reasonable endeavours to notify the Client of such activities.
- 3.6 The Parties expressly agree that, in the event of no written agreement between the Parties to the contrary, that no prior consent by the Client is required for JUMPSEC to install capabilities via the Agent such that the installed capabilities are solely to protect against likely or live cyber threats and attacks.

4. Maintenance Services

- 4.1 JUMPSEC will, during the term of this Service Specific Schedule, provide Maintenance Services to the Software.
- 4.2 JUMPSEC will, only upon the written request of the Client, notify the Client of any Maintenance Services to and of the Software.
- 4.3 In the event of no written request for the notification of Maintenance Services being received from the Client, JUMPSEC will be entitled to deliver any Maintenance Services that it deems necessary without the knowledge or prior consent of the Client.
- 4.4 The Client will promptly report any errors, faults or defects in the Software to JUMPSEC.

5. Restrictions of use of the Software

- 5.1 The Client will only be entitled to use the Software for its internal business purposes and will not permit any other person, save for the Authorised Users, to use the Software.
- 5.2 The Client may not, or cause any other person to

- 5.2.1 modify or reverse engineer the Software, or create derivative works of the Software;
- 5.2.2 sub-license the Software to third parties; or
- 5.2.3 use the Software outside of the permitted use of the Software as set forth in this Service Specific Schedule

6. Intellectual Property

- 6.1 The User acknowledges and agrees that JUMPSEC and/or its licensors own all rights to the Intellectual Property in the respective Software and the Documentation.
- 6.2 JUMPSEC may use ideas and feedback from the Client to improve the Software and/or the Documentation.
- 6.3 Except as expressly stated herein, JUMPSEC does not grant the User any Intellectual Property rights, other rights or licenses in respect of the Software and/or the Documentation.
- 6.4 The Client will own all Custom Detection rulesets and scripts, which shall be documented and maintained periodically throughout the Term and stored in a secure location accessible by the Client at any time.

Exit / Termination

Retention of Intellectual Property

Appendix B – Service Levels

This Service Level Agreement (SLA) forms part of the Master Agreement between JUMPSEC Ltd (the “Supplier”) and [Client Name] (the “Client”) for the provision of:

- i. Managed Detection and Response (MDR) Services
- ii. Continuous Attack Surface Management (CASM) Services

This SLA defines the agreed service levels, response times, availability, reporting requirements, and escalation procedures.

1. Definitions

“**Service Hours**” means the hours during which services are actively delivered.

“**Response Time**” – The time taken by JUMPSEC to acknowledge and commence investigation of an incident.

“**Resolution Time**” means the time taken to mitigate or remediate an issue, where feasible.

“**Priority Levels**” means the classification of security events or CASM findings based on urgency and impact.

“**Planned Maintenance**” means the Scheduled maintenance activities that may affect service availability.

“**Unplanned Outage**” means any unexpected service disruption.

2. Service Availability & Coverage

Service	Availability	Coverage
MDR	24x7x365	Full coverage including weekends and public holidays
CASM	09:00–17:00 GMT, Monday–Friday (excluding UK public holidays)	Standard business hours support

2.1. MDR services operate on a 24x7x365 basis, with continuous monitoring, detection, and response.

2.2. CASM services operate during business hours, with monitoring and reporting conducted within agreed schedules.

2.3. Service downtime due to planned maintenance shall be communicated at least 5 business days in advance.

2.4. The SLA commitments shall not apply in the event that:

- i. The Client fails to provide timely access to systems, logs, or personnel necessary for JUMPSEC to investigate security incidents.
- ii. The SLA failure is caused by a third-party provider, including but not limited to cloud services, ISPs, or external security vendors.
- iii. The security event is caused by pre-existing vulnerabilities, misconfigurations, or inadequate security measures on the Client's network.
- iv. The Client modifies, disables, or otherwise interferes with the security solutions deployed by JUMPSEC.

3. Incident Management & Response Times (MDR)

MDR service incidents are classified based on their severity and business impact, with the following response times, acknowledging that no resolution targets can be set:

Priority Level	Description	Response Time (Acknowledgement)
P1 – Critical		
P2 – High		
P3 – Medium		
P4 – Low		

- 3.1. The response time indicates when JUMPSEC will acknowledge and begin investigating the incident.
- 3.2. The resolution time is a target and depends on the complexity of the security event and required remediation.
- 3.3. For P1 incidents, JUMPSEC will maintain active engagement until containment and remediation are achieved.

4. CASM Service Deliverables & Response Times

- 4.1. CASM reports will be delivered on a scheduled basis, typically monthly, unless an urgent risk is identified.
- 4.2. Critical and High findings will be escalated immediately and addressed in collaboration with the Client's security team.

5. Escalation Process

If a response or resolution falls outside of SLA commitments, the following escalation path shall be followed:

Escalation Level	Contact	Timeframe
Level 1	MDR/CASM Operations Team	Immediate notification
Level 2	JUMPSEC Service Manager	Escalated within 2 hours
Level 3	JUMPSEC Security Leadership	Escalated within 6 hours
Level 4	Executive Management	Escalated within 24 hours

5.1. The Client may escalate any issue that remains unresolved beyond the defined resolution targets.

6. Service Reporting & Review

6.1 JUMPSEC will provide the following service reports:

Report Type	Frequency	Content
MDR Service Report	Monthly	Incident summaries, trends, response performance
CASM Service Report	Monthly	Risk analysis, findings, attack surface changes
Executive Security Review	Quarterly	Strategic insights, service impact, risk posture

6.2. Service review meetings will be conducted quarterly to discuss performance, trends, and continuous improvement.

7. Client Responsibilities

To ensure effective service delivery, the Client must:

- Provide relevant access to systems and log sources as agreed.
- Maintain up-to-date contact details for incident escalation.
- Respond to critical remediation recommendations within agreed timeframes.
- Ensure that JUMPSEC is notified of any changes to the IT environment that may affect monitoring.

Failure to meet these responsibilities may impact SLA performance.

8. Exclusions & Limitations

8.1 The SLA does not apply in the following cases:

- i. Client-caused delays (e.g., unavailability of contacts, lack of access).
- ii. Force Majeure events (natural disasters, large-scale internet outages).
- iii. Security events caused by pre-existing vulnerabilities that were not remediated following previous warnings.
- iv. Third-party actions outside of JUMPSEC's control.

8.2 JUMPSEC shall indemnify the Client only for fines, penalties, or regulatory sanctions directly attributable to JUMPSEC's failure to comply with its obligations as a Processor under GDPR.

8.3 JUMPSEC shall not be liable for any regulatory fines, legal costs, or penalties resulting from the Client's:

- i. Failure to obtain lawful basis for processing personal data.
- ii. Non-compliance with industry security standards.
- iii. Failure to implement recommended security measures that could have prevented a data breach.

Appendix C - Data Processing Agreement

This Data Processing Agreement (the "DPA") forms part of the Master Agreement between JUMPSEC Ltd ("Processor") and [Client Name] ("Controller") for the provision of cybersecurity managed services, specifically Detection, Response and Continuous Attack Surface Management (CASM) and consultancy.

This DPA ensures compliance with applicable data protection laws, including but not limited to the UK General Data Protection Regulation (UK GDPR), the EU General Data Protection Regulation (EU GDPR), and the UK Data Protection Act 2018.

1. Definitions

For the purposes of this DPA:

- "Controller"** means the entity that determines the purposes and means of the processing of personal data.
- "Processor"** means the entity that processes personal data on behalf of the Controller.
- "Sub-Processor"** means any third party engaged by the Processor to process personal data on behalf of the Controller.
- "Personal Data"** means any information relating to an identified or identifiable natural person that is processed by the Processor on behalf of the Controller under this DPA.
- "Processing"** means any operation or set of operations performed on personal data, including collection, storage, use, disclosure, or destruction.
- "Data Protection Laws"** means the UK GDPR, EU GDPR, Data Protection Act 2018, and any other applicable laws and regulations relating to the processing of personal data.

2. Subject Matter and Scope

- 2.1. The Processor shall process personal data only for the purposes of providing the following Managed Cyber Security Services under the Master Agreement:
 - i. Detection and Response Services
 - ii. Continuous Attack Surface Management (CASM)
- 2.2. The Processor shall process personal data only on documented instructions from the Controller, including in relation to transfers of personal data outside of the UK or EEA, unless required to do so by law.
- 2.3. The Processor shall not process personal data for any purposes beyond the agreed scope or for its own purposes.
- 2.4. Processor's Right to Refuse Non-Compliant Processing:

If the Client's processing instructions **contradict GDPR or other applicable data protection laws**, JUMPSEC shall:

- i. Immediately notify the Client of the potential legal conflict.
- ii. Refuse to process the data until legally compliant instructions are provided.

JUMPSEC shall not be liable for any delays, penalties, or legal claims resulting from the Client's failure to provide legally compliant instructions.

3. Categories of Personal Data and Data Subjects

3.1. Categories of Personal Data

The following types of personal data may be processed under this agreement:

- i. User identification data (e.g., usernames, email addresses, IP addresses)
- ii. Network traffic and security logs (may contain personal data in metadata)
- iii. Incident and security event data (may contain identifiers of affected individuals)
- iv. System access logs (potentially including timestamps, locations, and device details)

3.2. Categories of Data Subjects:

The processing activities may involve personal data of the following data subjects:

- i. Employees, contractors, and representatives of the Controller
- ii. Users and administrators of the Controller's IT infrastructure
- iii. Third parties interacting with the Controller's IT systems

4. Obligations of the Processor

The Processor shall:

4.1. Process personal data only on documented instructions from the Controller.

4.2. Ensure that persons authorised to process personal data are bound by confidentiality obligations.

4.3. Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including:

- i. Access controls to prevent unauthorised access to personal data
- ii. Encryption of data where applicable
- iii. Logging and monitoring of data access and processing activities
- iv. Regular security assessments and penetration testing

4.4. Assist the Controller in ensuring compliance with data protection impact assessments (DPIAs) where necessary.

4.5. Notify the Controller without undue delay (no later than 24 hours) upon becoming aware of a personal data breach, providing sufficient details and remedial actions.

4.6. Assist the Controller in responding to data subject rights requests (e.g., access, rectification, erasure) where applicable.

4.7. Ensure that all processing complies with applicable data protection laws.

5. Sub-Processing

5.1. The Processor shall not engage any sub-processor without prior written authorisation from the Controller.

5.2. If a sub-processor is engaged, the Processor shall ensure that the sub-processor is bound by the same data protection obligations as set out in this DPA.

5.3. The Processor remains fully liable for the actions of any sub-processor.

6. International Data Transfers

6.1. The Processor shall not transfer personal data outside of the UK or EEA without the Controller's written authorisation.

6.2. If an international transfer is required, the Processor shall:

- i. Ensure an adequacy decision is in place under UK GDPR/EU GDPR
- ii. Implement Standard Contractual Clauses (SCCs) or another valid mechanism
- iii. Apply appropriate safeguards to protect the data

7. Data Retention and Deletion

7.1. The Processor shall retain personal data only for the duration necessary to fulfil the purposes of the processing.

7.2. Upon termination of services, the Processor shall either delete or return all personal data to the Controller, unless required by law to retain it.

8. Liability and Indemnification

8.1. The Processor shall be liable for breaches of this DPA caused by its negligence, wilful misconduct, or failure to implement security measures.

8.2. The Processor shall indemnify the Controller against any fines, claims, or damages resulting from non-compliance to the extent that the Processor is responsible.

8.3. Liability shall be limited to the maximum liability stated in the Master Agreement, except in cases of wilful misconduct, gross negligence, or unlawful processing.

9. Audits and Compliance

9.1. The Processor shall maintain records of processing activities in accordance with Article 30 of GDPR.

9.2. The Controller may conduct an annual audit of the Processor's data processing activities, with prior notice, to assess compliance with this DPA.

9.3. The Processor shall provide evidence of compliance (e.g., certifications, audit reports, penetration testing results) upon request.

10. Term and Termination

10.1. This DPA shall remain in effect for the duration of the Master Agreement.

10.2. The Controller may terminate this DPA if the Processor is found to be in material breach of data protection obligations.

10.3. Upon termination, the Processor shall delete or return all personal data as outlined in Section 7.

11. Governing Law and Jurisdiction

11.1. This DPA shall be governed by and interpreted in accordance with the laws of England and Wales.

11.2. Any disputes shall be subject to the exclusive jurisdiction of the courts of England and Wales.

12. Signatures

For and on behalf of **JUMPSEC Ltd** (Processor):

Authorised Signatory	
Position / Title	
Date of Signature	
Signature	

For and on behalf of **[Client Name]** (Controller):

Authorised Signatory	
Position / Title	
Date of Signature	
Signature	