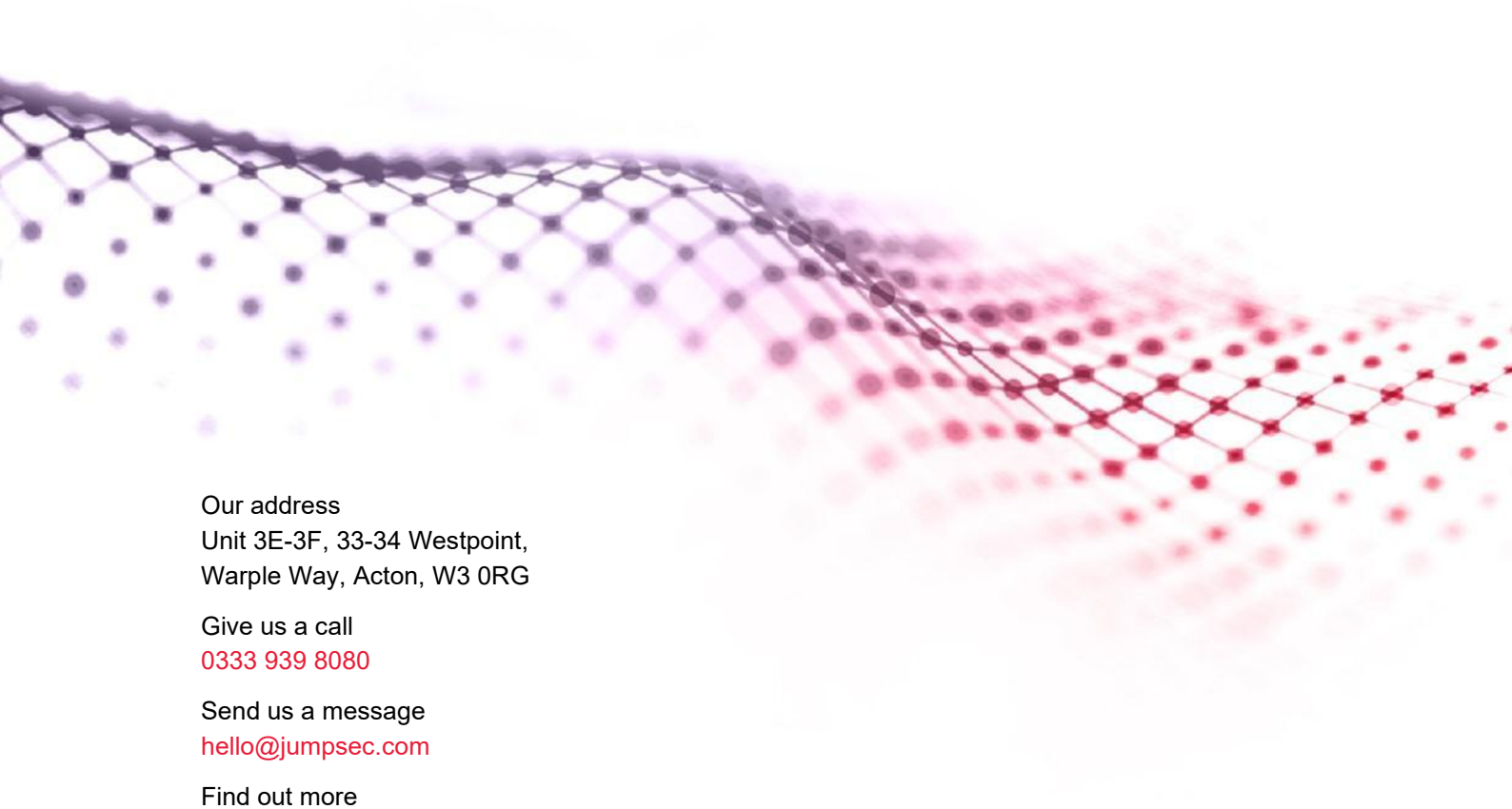
Service Specific Terms & DPA

JUMPSEC Services

V1.0



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

Give us a call
0333 939 8080

Send us a message
hello@jumpsec.com

Find out more
www.jumpsec.com

SERVICE SPECIFIC SCHEDULE – JUMPSEC Managed Services

This Service Specific Schedule for JUMPSEC Managed Services (Incident Response, MXDR, CASM) is entered into on the Go Live Date and are in addition to JUMPSEC's Standard Terms and Conditions v2.1. 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 Date specified in the Proposal and continue in full force and until the end of the Subscription per 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) or Proposal applicable to each service engagement.

3. 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 any software and reconfigure firewalls and other aspects of the Client's hardware, firmware and software, which were required 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.

4. 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.

5. 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.

6. Service Levels Incident Management & Response Times

Incident Response 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	Critical priority (P1) Incident investigation commenced.	Within 1 hour (including out-of-hours)
P2 – High	High priority (P2) Incident investigation commenced	Within 4 business hours
P3 – Medium	Medium priority (P3) Incident investigation commenced	Within 12 business hours
P4 – Low	Low priority (P4) Incident investigation commenced	Within 24 business hours

6.1. The response time indicates the maximum time taken for JUMPSEC to acknowledge and begin investigating the incident.

6.2. No Resolution Time is provided as resolution depends on the complexity of the security event and required remediation.

6.3. For P1 incidents, JUMPSEC will maintain active engagement until containment and remediation are achieved.

7. Client Responsibilities

7.1 To ensure effective service delivery, the Client must:

i. Provide relevant access to systems and log sources as agreed.

ii. Maintain up-to-date contact details for incident escalation.

iii. Respond to critical remediation recommendations within agreed timeframes.

iv. 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 [INSERT 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 in compliance with applicable data protection laws and any other relevant international transfer obligations;

iv. Ensure that any such transfers comply with the data protection and privacy laws applicable to both the Controller and the destination jurisdiction, including but not limited to those required under the UK GDPR, EU GDPR, and any other jurisdiction-specific requirements.

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. JUMPSEC shall indemnify the Client only for fines, penalties, or regulatory sanctions directly attributable to JUMPSEC's wilful misconduct or gross negligence in processing personal data. JUMPSEC shall not be liable for regulatory fines arising from:

i. The Client's failure to obtain lawful basis for data processing.

ii. The Client's failure to implement recommended security controls.

iii. Any security breach caused by third-party services beyond JUMPSEC's control, except where such third party is a sub-processor engaged by JUMPSEC in the provision of the Services, in which case JUMPSEC shall remain responsible for ensuring compliance with applicable data protection laws.

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 a maximum of 1 audit per calendar year, unless required by law or triggered by a security breach, and

i. The Client must provide at least 30 days' written notice before an audit.

ii. Audits must be conducted during business hours and shall not unreasonably disrupt JUMPSEC's operations.

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. Authorisation

	JUMPSEC (Processor):	**Client (Controller):**
Authorised Signatory Name		

Position / Title		
Date of Signature		
Signature		