SEP2 Wingman Terms and Conditions

January 2026

TECH DRIVEN.
PEOPLE POWERED.

TECH DRIVEN.
PEOPLE POWERED.

SEP2 Limited – Terms & Conditions

1. INTERPRETATION

1.1 The definitions in this clause apply in these terms and conditions:
Conditions: these terms and conditions, including (unless expressly stated otherwise) the applicable Service-Specific Schedules.
Contract: the contract between the Customer and the Supplier for the supply of Goods and/or Services created pursuant to clause 3 of these Conditions.
Contract Documents, Initial Contract Term and Contract Commencement Date: are defined in clause 2 of these Conditions.
Customer: the firm, company or other entity named as the customer in the Quotation.
Goods: the goods to be purchased by the Customer from the Supplier as described in the Quotation.
Quotation: a quote for the supply of Goods and/or Services issued by the Supplier to the Customer that is agreed between the parties pursuant to clause 2.1 of these Conditions.
Services: the services to be purchased by the Customer from the Supplier as described in the Quotation.
Service-Specific Schedules: the schedules attached to these Conditions which set out additional terms applying to some of the Supplier's service/product lines.
Supplier: SEP2 Limited, a company incorporated in England and Wales under number 09988870 whose registered office is at 51a St. Pauls Street, Leeds, England, LS1 2TE.

1.2 Unless the context otherwise requires, words in the singular shall include the plural and vice versa. A reference to writing or written includes email. References to clauses are to the clauses of these Conditions and references to paragraphs are to paragraphs of the relevant Service-Specific 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. CONTRACT FORMATION, COMMENCEMENT AND DURATION

2.1 The issue by the Supplier of a draft Quotation constitutes an offer to contract upon these Conditions, which may only be accepted by the Customer either signing the Quotation

where indicated (either by a “wet ink” signature or electronic signature via the Supplier’s contract management system) or, if it is not signed for any reason, by the Customer accepting the provision to it of any (or any part of) the Services or Goods described in the Quotation from the Supplier. Acceptance of the Quotation by the Customer as described above creates a Contract between the Customer and Supplier upon the terms of the most recent Quotation issued to the Customer prior to such acceptance, these Conditions and the applicable Service-Specific Schedules (together, “Contract Documents”). The date of the Customer’s signature on the Quotation, or the date of commencement of the provision of either Goods or Services to the Customer if there is no such signature, shall be the “Contract Commencement Date”. The parties may at any time mutually agree upon and enter into new or additional Contracts at any time.

2.2 The Contract shall commence on the Contract Commencement Date and shall continue for the period set out in the Quotation, unless terminated earlier in accordance with clause 9 (“Initial Contract Term”). If no such period is set out in the Quotation the Contract shall continue until completion of supply of the relevant Goods and/or Services.

2.3 Where the terms of any of the Contract Documents conflict, the terms contained in the documents listed higher in the list below shall take precedence:

2.3.1 Quotation;

2.3.2 Service-Specific Schedules; and

2.3.3 these Conditions.

2.4 The Contract Documents shall apply to govern the Contract, to the exclusion of any terms or conditions contained in, or referred to in, the Customer's purchase order, confirmation of order, specification or other documentation, and any such terms provided by the Customer shall not form part of or govern the Contract.

2.5 The Supplier shall use reasonable endeavours to perform its obligations under the Contract within the timeframes set out in the Quotation (if any). Time for performance of the Services or delivery of the Goods shall not be of the essence of the Contract.

2.6 The Service-Specific Schedules included in this Terms and Conditions will be reflective of the items and services within the Quotation.

2.7 Where the Contract is in respect of either support services or managed services or both (in each case as described further in the relevant Service-Specific Schedule), at the end of the Initial Contract Term, and on each anniversary thereafter, the Contract shall automatically renew for further successive periods of 12 months, unless either party gives written notice to the other to terminate the Contract in accordance with this clause. Any such notice must be served not less than 30 days prior to the end of the Initial Contract Term, or any anniversary thereof (as applicable), and such notice cannot expire prior to the end of the Initial Contract Term, or (as applicable) any anniversary thereof.

3. CUSTOMER'S OBLIGATIONS

3.1 The Customer shall:

3.1.1 co-operate with the Supplier in all matters relating to the Services and appoint a representative who shall have the authority to contractually bind the Customer on matters relating to the Contract (“Designated Contact”);

3.1.2 provide in a timely manner such access to the Customer's premises and data, and such office accommodation and other facilities, as requested by the Supplier. The Supplier will comply with the Customer's policies on access to the same that are provided to it in advance of such access. Where the provision of Goods or Services requires the Supplier's personnel to attend the Customer's premises, the Customer provide a safe working environment for this purpose;
3.1.3 provide in a timely manner such information as the Supplier may request, and ensure that such information is accurate in all material respects; and
3.1.4 be responsible (at its own cost) for preparing the relevant premises for receipt of the Goods/Services and for the provision of all necessary access and facilities reasonably required by the Supplier. If the Supplier is prevented from delivering on the agreed delivery date because no such preparation has been carried out, the Supplier may levy additional charges to recover any further costs incurred by it in relation thereto;
3.1.5 Obtain all necessary permissions and consents which may be required before the commencement of the Contract; and
3.1.6 Comply with such other requirements as may be set out in the Quotation or reasonably requested by the Supplier; and
3.1.7 In cases where any hardware items may be replaced through a RMA (Return Material Authorisation) Process, supply the Customer's Economic Operators Registration and Identification number (EORI number). Failure to supply EORI number may materially delay any delivery of replacement hardware items.
3.2 If the Supplier's performance of its obligations under the Contract is prevented or delayed by any act or omission of the Customer or the Customer's agents, subcontractors or employees, the Customer shall in all circumstances be liable to pay to the Supplier on demand all reasonable costs, charges or losses sustained or incurred by it.
3.3 The Customer warrants that it has the right, power and authority to enter into the Contract and to perform it in accordance with its terms.

4. CHARGES AND PAYMENT

4.1 Clause 4.2 shall apply if the Services are to be provided on a time-and-materials basis. Clause 4.3 shall apply if the Goods/Services are to be provided for a fixed price. The remainder of this clause 4 shall apply in either case.
4.2 Where the Services are provided on a time-and-materials basis:
4.2.1 the charges payable for the Services shall be calculated in accordance with the Supplier's standard daily fee rates as amended from time to time;
4.2.2 the Supplier's standard daily fee rates are calculated on the basis of an seven-hour working day worked between the hours of 8.00 am and 6.00 pm on weekdays (excluding weekends and public holidays);
4.2.3 the Supplier shall be entitled to charge at an overtime rate of 150% of the normal daily rate for part days and for time worked by the Supplier's personnel outside the hours referred to in clause 4.2.2 on a pro-rata basis;

4.2.4 the Supplier shall ensure that all Supplier personnel engaged in provision of the Services complete time sheets and shall record the total time spent on the Services, and the Supplier shall use such time sheets to calculate the charges; and
4.2.5 the Supplier shall invoice the Customer monthly for its charges for time, expenses and materials (together with VAT where appropriate) for the month concerned, calculated as provided in this clause 4.
4.3 Subject to any contrary provision in the Quotation, where the Goods and Services are provided for a fixed price, the price shall be the amount set out in the Quotation.
4.4 The Quotation will confirm whether the price of Goods and/or Services is payable in advance (or annually in advance) or in arrears. If the price is payable in advance, the Supplier shall not be obliged to commence work in respect of the Goods/Services to which the price relates, until payment has been made.
4.5 Any fixed price contained in the Quotation excludes:
4.5.1 the cost of hotel, subsistence, travelling and any other ancillary expenses reasonably incurred by the Supplier in connection with the Services;
4.5.2 any applicable delivery/shipping costs; and
4.5.3 VAT (value added tax),
which in each case the Supplier shall add to its invoices, and the Customer will pay (at the appropriate rate in respect of VAT).
4.6 Subject to any contrary provision in the Quotation, the Customer shall pay each invoice submitted to it by the Supplier in full, and in cleared funds, within 14 days of receipt. Time for payment shall be of the essence of the Contract.
4.7 Without prejudice to any other right or remedy that the Supplier may have, if the Customer fails to pay the Supplier on the due date the Supplier may:
4.7.1 charge costs and interest on such sums under the Late Payment of Commercial Debts (Interest) Act 1998 at the applicable rate from time to time in force. Interest shall accrue on a daily basis, and apply from the due date for payment until actual payment in full, whether before or after judgment; and
4.7.2 suspend all Services, and any further supply of Goods, until payment has been made in full.
4.8 All payments payable to the Supplier under the Contract shall become due immediately on termination of the Contract, notwithstanding any other provision.
4.9 All amounts due under the Contract shall be paid by the Customer to the Supplier in full without any set-off, counterclaim, deduction or withholding (other than any deduction or withholding of tax as required by law). The Supplier may, without prejudice to any other rights it may have, set off any liability of the Customer to the Supplier against any liability of the Supplier to the Customer.
4.10 For the avoidance of doubt, if the Supplier provides Goods or Services to the Customer at the Customer's request which are not referred to in a Quotation accepted by the Customer pursuant to clause 2.1 (but otherwise in accordance with these Conditions), the Supplier shall be entitled to invoice, and be paid by the Customer for, such Goods or Services.

4.11 If the Customer's procedures require that an invoice be submitted against a purchase order, the Customer shall be responsible for issuing such purchase order prior to the date of the Supplier's invoice.
4.12 The Supplier does not guarantee that the price of Goods or Services previously provided by it under any Contract shall be maintained in any subsequent Contract. Prices of Goods may change between orders, as may the Supplier's standard daily fee rates.
4.13 Where the Contract is in respect of either support services or managed services or both (in each case as described further in the relevant Service-Specific Schedule):
4.13.1 There shall be an automatic increase in the charges payable by the Customer no more than once in any 12 month period, of the higher of (i) 5%, or (ii) the percentage increase, over the preceding 12 months for which figures are available, in the UK RPI (For the purposes of this clause, "RPI" means the retail prices index used as a measure of inflation in the UK which is published and updated by the Office for National Statistics from time to time); and
4.13.2 Prior to any renewal of the Contract pursuant to clause 2.7, the Supplier may propose an additional price increase (notwithstanding the automatic price increase under clause 4.13.1) to apply as from the end of the Initial Contract Term, and/or subsequently upon any anniversary thereof, on notice to the Customer not less than 60 days prior to the end of the Initial Contract Term, or (as applicable) any anniversary thereof. Subject always to the Customer's right to terminate the Contract under clause 2.7, any such proposed price increase shall automatically apply (and the charges shall be adjusted accordingly) as from the end of the Initial Contract Term, or (as applicable) any anniversary thereof.

5. THIRD PARTY SOFTWARE

5.1 Where the Supplier supplies third party software (whether provided via a licence key or access to a portal or otherwise), the Customer's right to use such software is subject to the relevant software licensor's end user licence agreement ("EULA") in respect of such software, which the Customer shall comply with in full. The EULA may be made available on a 'click-wrap', 'shrink-wrap' or other similar basis, or otherwise available from the Supplier on request. The Customer acknowledges and agrees that it shall have no greater rights or remedies against the Supplier in respect of such software, as the Supplier has against the vendor of such software.

5.2 Service Specific Schedules may contain additional Third Party Software clauses relevant to the specific services being delivered, and in some cases the Quotation will also include any specific Third Party Software Clauses relevant to the sale, resale or use of Third Party Software as part of a Wingman Service deliverable.

6. INTELLECTUAL PROPERTY RIGHTS

6.1 Nothing in the Contract shall operate to transfer any existing intellectual property rights from one party to the other, unless otherwise specifically identified in the Quotation. Any new intellectual property rights created by the Supplier in the course of the Contract shall vest in the Customer upon creation, unless specifically agreed otherwise in the Quotation.

7. CONFIDENTIALITY

7.1 Any party (the "Receiving Party") shall keep in strict confidence all technical or commercial know-how, specifications, inventions, processes or initiatives which are of a confidential nature and have been disclosed to it by the other party (the "Disclosing Party"), its employees, agents or sub-contractors and any other confidential information concerning the Disclosing Party's business or its products which the Receiving Party may obtain. The Receiving Party shall restrict disclosure of such confidential material to such of its employees, agents or sub-contractors as need to know the same for the purpose of discharging the Receiving Party's obligations under the Contract, and shall ensure that such employees, agents or sub-contractors are made aware of the confidential nature of such confidential material.

8. LIABILITY

8.1 Nothing in the Contract excludes the liability of the Supplier for anything which cannot be excluded under applicable law.

8.2 All Services will be provided using reasonable care and skill. Subject to the foregoing, all warranties, conditions and other terms implied by statute or common law are, to the greatest extent permitted by law, excluded from the Contract. Without limitation to the foregoing, the Supplier does not warrant that use of any Goods or third party software shall meet the Customer's expectations or work as intended with any of the Customer's other hardware or software, and the Supplier has no liability to the Customer in respect thereof where the Customer's requirements have not been sufficiently brought to the Supplier's attention prior to the Contract or where the Customer has not followed the Supplier's express advice.

8.3 Subject to clauses 8.1 and 8.2:

8.3.1 the Supplier shall not in any circumstances be liable, whether in tort (including for negligence or breach of statutory duty however arising), contract, misrepresentation (whether innocent or negligent) or otherwise for:

8.3.1.1 loss of profits;

8.3.1.2 loss of business;

8.3.1.3 depletion of goodwill or similar losses;

8.3.1.4 loss of anticipated savings;

8.3.1.5 loss of contract;

8.3.1.6 loss of use;

8.3.1.7 loss or corruption of data or information; or
8.3.1.8 any special, indirect, consequential or pure economic loss, costs, damages, charges or expenses.
8.3.2 the Supplier shall not in any circumstances have any liability to the Customer if it is prevented from, or delayed in, performing its obligations under the Contract as a result of any act or omission of the Customer, its employees, agents or sub-contractors, and any timescales for provision of the Services shall be amended accordingly.
8.3.3 the Supplier's total liability in contract, tort (including negligence or breach of statutory duty however arising), misrepresentation (whether innocent or negligent), restitution or otherwise, arising in connection with the performance or contemplated performance of the Contract shall be limited to either (i) in the first year of the Contract, a sum equal to the total price set out in the initial agreed Quotation, or (ii) in the second and any subsequent year of the Contract, a sum equal to the total charges actually paid by the Customer to the Supplier under the Contract in the 12 month period immediately preceding the date of the relevant liability arising.
8.4 The Customer shall indemnify and keep indemnified in full (and on demand) the Supplier against all claims, costs and expenses which the Supplier may incur and which arise, directly or indirectly, from:
8.4.1 the Customer’s breach of any of its obligations under the Contract;
8.4.2 any breach of third party intellectual property rights arising from the Supplier’s compliance with the Customer’s instructions or from the Supplier’s reconfiguration of Goods or software in accordance with the Customer’s specification; and
8.4.3 any failure by the Customer to enter into any end user licence agreement required in respect of any third party software that is identified in the Quotation as being part of this Contract of supply.

9. TERMINATION

9.1 Without prejudice to any other rights or remedies to which the parties may be entitled, either party may terminate the Contract without liability to the other if:
9.1.1 the other party fails to pay any amount due under the Contract on the due date for payment and remains in default not less than 7 days after being notified in writing to make such payment;
9.1.2 the other party commits a material breach of any other term of the Contract, which breach is irremediable or (if such breach is remediable) fails to remedy that breach within a period of 14 days after being notified in writing to do so;
9.1.3 the other party convenes a meeting of its creditors or makes or proposes any arrangement or composition with, or any assignment for the benefit of its creditors;
9.1.4 an order is made by a court of competent jurisdiction or a resolution is passed for the dissolution, winding-up or administration of the other party (other than due to a solvent restructuring);
9.1.5 if a trustee, receiver, administrator or other similar officer is appointed in respect of all or any part of the other party’s business; or

9.1.6 the other party is or becomes unable to pay its debts within the meaning of s.123 of the Insolvency Act 1986.
9.2 Any provision of the Contract that expressly or by implication is intended to come into or continue in force on or after termination or expiry of it shall remain in full force and effect. Termination of the Contract shall not affect any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination.

10. FORCE MAJEURE

10.1 The Supplier shall not in any circumstances have any liability to the Customer under the Contract if it is prevented from, or delayed in, performing its obligations under the Contract or from carrying on its business due to any act, event, omission or accident outside of the Supplier's reasonable control including, without limitation strikes, lock-outs or other industrial disputes (whether involving the workforce of the Supplier or any other party); failure of a utility service or transport network; power failure; internet downtime or available bandwidth shortage; act of God, war, riot or civil commotion; malicious damage; pandemic; compliance with any law or governmental order, rule, regulation or direction; and accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or subcontractors.

11. DATA PROTECTION

11.1 For the purposes of this clause 11, "controller", "processor", "data subject", "personal data", "personal data breach", "processing" "process" and "appropriate technical and organisational measures" shall have the meanings given to them in the Data Protection Legislation. "Data Protection Legislation" means all applicable data protection and privacy legislation in force from time to time in, or applicable in, the UK including the retained EU law version of the General Data Protection Regulation ((EU) 2016/679)) (UK GDPR); the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.
11.2 The Supplier and Customer shall comply with all applicable requirements of the Data Protection Legislation. This clause 11 is in addition to, and does not relieve, remove or replace, a party's obligations or rights under the Data Protection Legislation.
11.3 Where the Supplier processes any personal data disclosed by the Customer as a data controller in the performance of its obligations under the Contract, such personal data shall be processed in accordance with the Supplier's privacy and GDPR policy which can be accessed at https://www.sep2.co.uk/gdpr and https://www.sep2.co.uk/PrivacyPolicy respectively.
11.4 The Supplier processes personal data as a processor on behalf of the Customer. The supplier agrees to process personal data in accordance with this clause 11.4

11.5 By becoming a customer, you agree to receive our monthly newsletter containing updates and insights related to our services. You can unsubscribe at any time using the link provided in each email.

Instructions

Supplier shall only process (and shall ensure its employees and personnel only process) the personal data in accordance with all applicable Data Protection Legislation and this Agreement, (unless alternative processing instructions are agreed between the parties in writing).

Security

Supplier shall implement and maintain appropriate technical and organisational measures to protect the personal data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access. On overview of the details of these technical and organisational measures are available to view at https://trust.sep2.security

Sub-Processing

The Supplier shall not permit sub-processing of personal data without the prior written consent of the Customer.

1. prior to any sub-processor carrying out any processing activities in respect of the personal data, the Supplier shall appoint each sub-processor under a written contract containing materially the same obligations in respect of processing of personal data as under this Agreement that is both compliant with applicable Data Protection Legislation and enforceable by Supplier and ensure each such sub-processor complies with all such obligations;
2. remain fully liable to the Customer for all the acts and omissions of each sub-processor as if they were its own;
3. ensure that all persons authorised by Supplier or any sub-processor to process the personal data are subject to a binding written contractual obligation to keep the personal data confidential; and
4. inform the Customer of any intended changes concerning the addition or replacement of any sub-processor with at least 30 days' prior written notice of such anticipated change, thereby giving the Customer the opportunity to object to such changes.

SEP2 provide a list of sub-processors available to view at https://trust.sep2.security

Assistance

Supplier shall:

Assist the Customer in ensuring compliance with the Customer's obligations pursuant to UK GDPR and any data protection impact assessments (and any similar obligations under applicable Data Protection Legislation) taking into account the nature of the processing and the information available to the Supplier; andtaking into account the nature of the processing, assist the Customer (by appropriate technical and organisational measures), insofar as this is possible, for the fulfilment of the Customer's obligations to respond to requests for exercising the Data Subjects' rights under Chapter III ("Rights of the data subject") of the UK GDPR (and any similar obligations under applicable Data Protection Legislation) in respect of any personal data.

International transfers

Supplier shall not Process and/or transfer, or otherwise directly or indirectly disclose, any personal data in or to countries outside the United Kingdom and European Economic Area without the Customer's prior written consent and in any event in compliance with applicable Data Protection Legislation.

Audit

Supplier shall, in accordance with applicable Data Protection Legislation, make available to the Customer such information as is reasonably necessary to demonstrate the Customer's compliance with the obligations placed on it under both applicable Data Protection Legislation and this Agreement, and allow for and contribute to audits, including inspections, by the Customer.

Breach

Supplier shall notify the Customer without undue delay and in any event in compliance with applicable Data Protection Legislation and in writing on becoming aware of any personal data breach.

Deletion/return

Upon termination of the Agreement, and therefore at the end of the need to process any personal data, at the Customer's option, Supplier shall either return all of the Personal data to the Customer or securely dispose of the personal data (and thereafter promptly delete all existing copies of it) except to the extent that any applicable law or reasonable audit procedures require Supplier to store such personal data, and confirm to the Customer in writing that it has complied with this obligation.

12. NOTICES

12.1 Any notice given under this Contract shall be in writing and shall be delivered either:

12.1.1 by sending it by first class, registered post to the other party at its address set out in this Contract (or such other address as may be notified by it in writing to the other party from time to time); or

12.1.2 by email to:

12.1.2.1 contracts-support@sep2.co.uk for the Supplier, and

12.1.2.2 The email address for the Customer shown in the Quotation.

12.2 Any notice which is sent by post shall be deemed to have been received 2 working days after posting, or if sent by email shall be deemed to have been received at 9 am on the working day after it was sent, provided it was sent on a working day (or at 9am on the 2nd working day after it was sent if not sent on a working day) and provided in each case that the sender has not received a notice of send failure from its email system.

13. GENERAL

13.1 Waiver. No failure or delay by a party to exercise any right or remedy provided under this agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single

or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

13.2 Severance. If any provision or part-provision of the Contract is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this agreement. The parties shall negotiate in good faith to amend such provision so that, to the greatest extent possible, the amended provision achieves the intended commercial result of the original provision.

13.3 Variation. No addition to, variation of, exclusion or attempted exclusion of any term of the Contract shall be binding on the Supplier unless in writing and signed by a duly authorised representative of the Supplier.

13.4 Entire agreement. The Contract 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. In entering into the Contract, the Customer does not rely on, and shall have no remedies in respect of, any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in the Contract, and the Customer shall have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in the Contract.

13.5 Assignment. The Customer shall not, without the prior written consent of the Supplier, assign, transfer, charge, subcontract, delegate, declare a trust over or deal in any other manner with all or any of its rights or obligations under the Contract. The Supplier may at any time assign, transfer, charge, subcontract, delegate, declare a trust over or deal in any other manner with all or any of its rights or obligations under the Contract.

13.6 No partnership or agency. Nothing in the Contract is intended to or shall operate to create a partnership between the parties, or to authorise either party to act as agent for the other, and neither party shall have authority to act in the name or on behalf of or otherwise to bind the other in any way.

13.7 Third party rights. The Contract does not give rise to any rights under the Contracts (Rights of Third Parties) Act 1999 to third parties to enforce any term of the Contract.

13.8 Governing Law & Jurisdiction. The Contract and any disputes or claims arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) are governed by and construed in accordance with the laws of England and Wales. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with the Contract or its subject matter or formation (including non-contractual disputes or claims).

13.9 Non-poaching. The Customer shall not, without the prior written consent of the Supplier, at any time from the Contract Commencement Date to the expiry of 12 months after termination of the Contract, solicit or entice away from the Supplier or employ or attempt to employ any person who is, or has been, engaged as an employee or subcontractor of the Supplier. The Customer shall not be in breach of this clause 13.9 if it hires an employee or subcontractor of the Supplier as a result of a recruitment campaign not specifically targeted to any employees or subcontractors of the Supplier.

TECH DRIVEN.
PEOPLE POWERED.

TECH DRIVEN.
PEOPLE POWERED.

SERVICE-SPECIFIC SCHEDULE: MANAGED SERVICES ("Wingman MDR")

Where the Supplier provides a 'managed service' to the Customer, the following terms shall apply.

1. PROVISION OF MANAGED SERVICES

1.1 The Supplier shall provide managed services only in respect of the goods/software/equipment supplied by the Supplier (or as otherwise expressly identified in the Quotation).

1.2 The Supplier does not warrant that the Supplier's provision of, and the Customer's use of, the managed services will be uninterrupted or error-free.

Wingman MDR Standard Includes:

1.3 **Deployment of the Service**, in accordance with section 4 of this Service Specific Schedule

1.3.1 **Creation of content** within the Google SecOps platforms, including but not limited to YARA-L detection rules, SIEM Dashboards & SOAR playbooks. The content will be defined during the deployment and through ongoing service review meetings, as well as in reaction to events and detections found and "real world" events that may make specific need of specific content. There shall be no limit to the amount of content created. The Customer can request content to be made to make the service more tailored to their specific needs, and so long as the Content can be made, it shall be.

1.3.2 **Enrich alerts** with automated tooling and Threat Intelligence platforms to be able to provide more contextual information within the alert or event to aid in the delivery of the Service.

1.3.3 **Investigating alerts** that the Service generates. This will include both automated (by the technology) and human-led (by SEP2 employees) investigating the events which have been detected and understanding what has been detected, delivered by our staffed 24/7/365 SOC in Leeds, UK.

1.3.4 **Respond to events** using the integrations that have been facilitated as part of the deployment within the system, be able to automate or manually respond to events and take preventative and reactive actions within the Customers environment, within permitted scope as part of the defined operational handbook.

1.3.5 **Complete Threat Hunts** where SEP2 Security Analysts, using Threat Intelligence as well as their specific knowledge, complete proactive searches within the Service to identify any areas of concern that the platform had not detected automatically. Create feedback loops to then bring the outcomes of the Threat Hunt into detection content
1.3.6 **Capture the service boundaries** and engagement methodologies within the operational handbook, which is a living document that will be created during the onboarding and will be the source of truth as to the limit of scope and function that the Supplier will do.
1.3.7 **Create Service Reports** as defined within section 5 of this Service Specific Schedule, create and deliver the required service reports and service review meetings to be able to validate to the Customer that the service is being delivered in the way in which it should be, and to allow for the opportunity for the Customer and the Supplier to feedback to each other.
1.3.8 **Change management** – to ensure that the Service is adapting to the Customers changing environment, the Supplier shall use best endeavours to comply with day-to-day changes to the Customer's environment as requested by the Customer's employees ("Change Requests") in accordance with the target response times in the table below provided always that such Change Requests are limited to the features of the relevant equipment and service supplied by the Supplier, and the Supplier has sufficient resources available to comply with such Change Requests. In the table below, "Action" means that an engineer will review the change request and either complete the change as requested or respond to the requestor of the change seeking further information necessary to complete the change.

PRIORITY	DESCRIPTION	RESPONSE TIME (FOR RECEIPT OF CHANGE REQUEST)
1. Urgent	Change required in order to provide a workaround for a critical issue	Action within 2 hours
2. Unplanned	Ad-Hoc change that is not part of a pre-defined project	Action within 8 working hours
3. Planned	Change as part of a pre-defined project	Action within 24 working hours

Wingman MDR Enhanced Adds:

1.3.9 **Digital Threat Monitoring** - Using the Google Threat Intelligence platform, the Supplier will create monitors in the DTM platform to monitor the deep and dark web for specific mentions of relevant IP addresses, URL's, domain names, VIP user names and other Customer specific information as agreed. Triggers of these monitors will open cases aligned with the SLA as provided in clause 3 of this Service Specific Schedule.

1.3.10 **Attack Surface Management** - Using the Google Threat Intelligence Platform, the Supplier will create Attack Surface Management projects and scopes to provide for visibility of the Customers Attack Surface. Critical detections from the ASM platform will trigger a case aligned with the SLA as provided in clause 3 of this Service Specific Schedule.

1.3.11 **Threat Profiling** - Using the Google Threat Intelligence Platform, the Supplier will create a customised Risk Profile aligned to the Customers specific industry and geographics of operation, to use as part of the delivery of the Wingman MDR service.

1.3.12 **Mandiant Emerging Threat Detections** - The Mandiant Emerging Threat Detections feed will be enabled within the Google SecOps platform for the Customer to provide a higher fidelity set of Threat Intelligence to use as part of the delivery of the Wingman MDR service.

2. CUSTOMER OBLIGATIONS

2.1 The Customer shall not store, distribute or transmit any material on its systems in respect of which managed services are provided by the Supplier that:

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

2.1.2 facilitates illegal activity;

2.1.3 depicts sexually explicit images and/or

2.1.4 promotes unlawful violence, discrimination based on race, gender, age, disability, sexual orientation, religion, belief or gender reassignment, or any other illegal activity.

3. SUPPORT TICKETS AND SERVICE LEVELS AGREEMENTS

3.1 The Customer may log any issues with the Supplier by telephone, email or web-portal ("Support Ticket") which shall be dealt with by the Supplier in accordance with the service levels identified in the table below.

3.2 Events or Alerts that the Service generates will, through consultation of the operational handbook and the Suppliers best industry knowledge, will be graded into the SLA service levels below.

3.2 The response and escalation times are dependent on the severity level of the Support Ticket as set out in the table below. Upon logging a Support Ticket with the Supplier's Support Engineer, an initial assessment shall be undertaken by the Supplier and a severity level discussed and agreed. The Customer should retain a record of any Support Ticket number which may be provided by the Support Engineer.

SEP 2

TECH DRIVEN.
PEOPLE POWERED.

SERVICE LEVEL	DESCRIPTION	HOURS OF COVER	RESPONSE TIME	SEP2 INTERNAL ESCALATION ROUTE	ESCALATION PATHWAY TO CUSTOMER
1	**Platform / Service Impact** System Down. Production service or other mission-critical system(s) are down and no workaround is immediately available. This will impact all users **Defined / Understood Security Incidents** High confidence/severity threat that if confirmed and uncontained is likely to have a significant impact to the Confidentiality, Integrity or Availability of one or more of the customer's production systems. **24/7 Analyst Led Awareness / Areas of Interest** Repeated instances of potentially related but disparate security detections have occurred that warrant a severity 1 response and further analysis	7 days a week 24 hours a day 24 x 7	SEP2 SOC team consolidate and verify event information and provide initial analysis within 15 minutes of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 Specialist SecOps team if further technical input or analysis is required or if the original issue is outstanding after 30 minutes. SEP2 Specialist SecOps team escalates to Google Support in cases of Platform issues. Ongoing escalation and SLA as per Google SLA (https://cloud.google.com/terms/secops/sla)	In cases triaged and identified as False Positive, notification / escalation is not performed but is included in service reporting / dashboards for visibility. Active / ongoing Severity 1 issues notified to customer either at pre-determined point in agreed playbook or as needed on the basis of SEP2 requiring the customer to take remedial/preventative/further actions themselves, or to provide further additional business context that may be required.
2	**Platform / Service Impact** System is operating a degraded service to all users. One of more subsystems are not	7 days a week 24 hours a	SEP2 SOC consolidate and verify event	SEP2 SOC escalate to SEP2 Specialist SecOps if further technical	In cases triaged and identified as False Positive, notification / escalation is not performed

	functioning or are impacting only a subset of users. **Defined / Understood Security Incidents** Medium confidence/severity threat that if confirmed and uncontained could impact the Confidentiality, Integrity or Availability of one or more of the customer's production systems. **24/7 Analyst Led Awareness / Areas of Interest** Repeated instances of potentially related but disparate security detections have occurred that warrant a severity 2 response and further analysis.	day 24 x 7	information and provide initial analysis within 1 hour of initial report and begin further investigations or remedial actions as soon as technically able.	input or analysis is required or if the original issue is outstanding after 60 minutes. SEP2 Specialist SecOps team escalates to Google Support in cases of Platform issues. Ongoing escalation and SLA as per Google SLA (https://cloud.google.com/terms/secops/sla)	but is included in service reporting / dashboards for visibility. Active / ongoing Severity 2 issues notified to customer either at pre-determined point in agreed playbook or as needed on the basis of SEP2 requiring the customer to take remedial/preventative/further actions themselves, or to provide further additional business context that may be required.
3	**Platform / Service Impact** All major functionality is working. Non-critical system issues. Impaired operations of some components but allows the user to continue using the system. **Defined / Understood Security Incidents** A low confidence action, that under many scenarios will be non-malicious and requires additional context to verify if	7 days a week 24 hours a day 24 x 7	SEP2 SOC consolidate and verify event information and provide initial analysis within 4 hours of initial report and begin further investigations or remedial actions	SEP2 SOC escalate to SEP2 Specialist SecOps team if further technical input or analysis is required or if the original issue is outstanding after 8 hours. SEP2 Specialist SecOps team escalates to Google Support in	In cases triaged and identified as False Positive, notification / escalation is not performed but is included in service reporting / dashboards for visibility. Active / ongoing Severity 3 issues notified to customer either at pre-determined point in agreed playbook or as needed on the basis of SEP2

	malicious intent has occurred.		as soon as technically able.	cases of Platform issues. Ongoing escalation and SLA as per Google SLA (https://cloud.google.com/terms/secops/sla)	requiring the customer to take remedial/preventative/further actions themselves, or to provide further additional business context that may be required.
4	**Platform / Service Impact** General enquiries. No service degradation. **Defined / Understood Security Incidents** A high volume alert that is a known false positive, that poses little or no security risk and that has not yet been remediated or tuned.	7 days a week 24 hours a day 24 x 7	SEP2 SOC consolidate and verify event information and provide initial analysis within 8 hours of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 Specialist SecOps team if further technical input or analysis is required or if the original issue is outstanding after 24 hours.	No escalation of this severity of issue to the customer is performed, but statistics and information on these events are included in reporting and are available in the SOAR dashboards.

4. SERVICE DEPLOYMENT

4.1 A planning session will be held between the Supplier and the Customer where specific requirements are captured and a working implementation plan is developed and agreed upon, as well as mutual agreement by both the Supplier and Customer as to timelines, milestones, and key dates to achieve transition to “live”. Neither party shall be unreasonable in providing agreement and sufficient resources to ensure that the timelines agreed are achievable.

4.1.1 The default deployment method will be for a SecOps SIEM instance to be created in the EU-MultiRegion as defined at https://cloud.google.com/terms/secops/data-residency?hl=en unless the Quotation provides a more specific region. SecOps SOAR will be an environment within the SEP2 MSSP SOAR platform which is hosted in Europe-West-2 (London, UK).
Key elements which must be agreed during this scoping session may include, but are not limited to:
4.1.1 Log Source prioritised list and identified collection mechanism which defines what the Live service will be
4.1.2 Chronicle Collector / Bindplane virtual machine / docker environment
4.1.3 Development of the Operational Handbook and Playbooks to facilitate case handling and investigation functions and reactive response components

4.2 The Supplier makes use of a project management tool, Halo, which it will allow the Customer access to, to be able to track and manage the process of the implementation. Exports from Halo can be taken via CSV/Excel as needed should the Customer need to manage data in their own environment.
4.2.1 The Supplier may use alternative specific tools from time to time at their discretion, so long as suitability of tools is largely inline with the functions that Halo provide.

4.2.2 After the planning and scoping session, the specific agreed tasks and milestones, capturing resourcing requirements from both the Supplier and the Customer will be added into the Halo project.

4.3 Deployment of Chronicle Log Collector or Bindplane platforms within the Customers network is dependent on the Customer providing sufficient access to create virtual machines or docker instances, or allowing the agents to be run on already existing infrastructure.

4.4 The configuration of the Log Sources will be implemented as per the prioritised list defined and agreed within the scoping session.

4.5 The Customer will ensure that they make available to the Supplier suitably experienced and authorised personnel to be able to facilitate the service implementation, considering required authentication and access to log sources and ability to enact changes as needed to facilitate log source onboarding.

4.6 During the service implementation phase, and subject to mutual agreement to change the frequency, a weekly update meeting will be held. The scope of that meeting is from a project management perspective, to ensure that the deployment is being completed as per the agreed plan created within the planning and scoping session.

4.6.1 Should any issues, dependencies, problems or other such be identified within this meeting, the respective party (either the Customer or the Supplier) will endeavor to provide further details and plans on how that can be remediated.
4.6.2 At a point which is mutually agreed upon by both the Supplier and the Customer, this scheduled update meeting can be stopped, at which point the service is deemed to have been deployed to live stage, and the service has entered into the business as usual phase.

4.7 During the implementation phase and thereafter as needed, the Supplier and the Customer will make use of the best possible methods of shared and communal communication, such as a shared Teams, Slack or Google Chat channel.

5. REPORTING & BUSINESS CONTINUITY

5.1 The Supplier shall provide reports to the Customer which summarises the Services provided to the Customer in the previous 90 days, on a rolling 90 day basis. Notwithstanding the foregoing, the Supplier and Customer shall have Service review meetings at a location to be mutually agreed on a rolling 90 day basis. The Service review meetings shall be attended by key contacts of both the Supplier and Customer to be mutually agreed in advance. The purpose of the Service review meetings is to allow either party to provide feedback on the Services.
5.2 The Supplier shall implement a disaster recovery plan which sets out the Supplier's approach to ensure business continuity for the Services. The Supplier shall regularly carry out testing of its procedures for this purpose

6. SERVICE HANDOVER / EXIT TRANSITION

6.1 Irrespective of the methodology or reasons why a Termination (Clause 9 of the Terms and Conditions) has occurred, or in the case where the Contract is in its final month and is not intended to be extended/renewed by the Customer, the Supplier warrants that it shall act reasonably and with good faith to help and facilitate the Customer in the actions which may be required to support the Customer in moving to an alternative provider or platform.
6.2 Any content created in the SecOps SIEM or SOAR platforms that is specific to the Customer (parsers, rules, detections, dashboards, playbooks etc) will be available for the Customer to continue to use or export as part of the exit process.
6.3 Should the Customer wish to export log-data from within the Google SecOps platform to any other environments, the Customer will provide to the Supplier Google Cloud Storage Account (which, for the avoidance of doubt, will be owned and paid for by the Customer). Under direction by the Customer as to the specifics as to what log-data to export to the Google Cloud Storage Account, the Supplier will facilitate the export of that data and will assist the Customer in understanding the potential costs associated with the underlying Google Cloud Storage Account.

7. THIRD PARTY SOFTWARE

7.1 Google SecOps is part of the wider Google Cloud Platform, and therefore the terms and conditions of use of Google Cloud Platform are within the scope of these terms. Specifically, the following terms are within the EULA - https://cloud.google.com/product-terms (tick the SecOps Services filter to see the specific terms as relevant, including but not limited to:)

- “SecOps Service URL Terms > Acceptable Use Policy”
- “SecOps Service URL Terms > Cloud Data Processing Addendum (Customers)”
- “SecOps Service URL Terms > Service Specific Terms”
- “SecOps Service URL Terms > Service Level Agreements”
- “SecOps Service URL Terms > Technical Support Services Guidelines”
- “Other SecOps Services Resources > SecOps Privacy Notice”
- “Other SecOps Services Resources > Services Summary”
- “Other SecOps Services Resources > Services in Scope by Compliance Program”
- “Other SecOps Services Resources > Subprocessors”

TECH DRIVEN.
PEOPLE POWERED.

SERVICE-SPECIFIC SCHEDULE: MANAGED SERVICES ("Wingman EDR")

Where the Supplier provides a 'managed service' to the Customer, the following terms shall apply.

1. PROVISION OF MANAGED SERVICES

1.1 The Supplier shall provide managed services only in respect of the goods/software/equipment supplied by the Supplier (or as otherwise expressly identified in the Quotation).

1.2 The Supplier does not warrant that the Supplier's provision of, and the Customer's use of, the managed services will be uninterrupted or error-free.

Wingman EDR Basic Includes:
1.3 **Deployment of the Service**, in accordance with section 4 of this Service Specific Schedule
1.3.1 **Enrich alerts** with automated tooling and Threat Intelligence platforms to be able to provide more contextual information within the alert or event to aid in the delivery of the Service.
1.3.2 **Policy Management** - Configure the EDR platform technology policy in accordance with Customer needs and with consideration to best industry practise.
1.3.3 **Endpoint Troubleshooting** - Complete relevant and appropriate troubleshooting with the Customer and the Customer users to resolve problems identified, in alignment with the SLA table component "Platform / Service Impact" only in section 3 of this Service Specific Schedule.
1.3.4 **Vendor Issue Escalation** - In cases where troubleshooting and policy management cannot resolve an issue, the Supplier will escalate to the Vendor for Vendor support as required.
1.3.5 **Change management** – to ensure that the Service is adapting to the Customers changing environment, the Supplier shall use best endeavours to comply with day-to-day changes to the Customer's environment as requested by the Customer's employees ("Change Requests") in accordance with the target response times in the table below provided always that such Change Requests are limited to the features of the relevant equipment and service supplied by the Supplier, and the Supplier has sufficient resources available to comply with such

Change Requests. In the table below, “Action” means that an engineer will review the change request and either complete the change as requested or respond to the requestor of the change seeking further information necessary to complete the change.

PRIORITY	DESCRIPTION	RESPONSE TIME (FOR RECEIPT OF CHANGE REQUEST)
1. Urgent	Change required in order to provide a workaround for a critical issue	Action within 2 hours
2. Unplanned	Ad-Hoc change that is not part of a pre-defined project	Action within 8 working hours
3. Planned	Change as part of a pre-defined project	Action within 24 working hours

Wingman EDR Standard adds:

1.3.6 **Automated Threat Investigation** - leveraging the technology, investigating the events which have been detected and understanding what has been detected.

1.3.7 **Automated Threat Response** - using the integrations that have been facilitated as part of the deployment within the system, be able to automate response to events and take preventative and reactive actions within the Customers environment, within permitted scope as part of the defined operational handbook.

1.3.8 **Human eyes-on Threat Confirmation** - leveraging our 24/7/365 SOC based in Leeds, UK, our analyst team provides eyes-on response and validation to the events that are detected by the platform, as aligned with the SLA table component “Defined / Understood Security Incidents” and “24/7 Analyst Led Awareness / Areas of Interest” in section 3 of this Service Specific Schedule.

Wingman EDR Enhanced adds:

1.3.9 **Detailed Threat Investigation** - Our threat response team within our 24/7/365 take further detailed investigation tasks and pivot searching to be able to validate an event in more detail.

1.3.10 **Threat Hunting** - where SEP2 Security Analysts, using Threat Intelligence as well as their specific knowledge, complete proactive searches within the Service

to identify any areas of concern that the platform had not detected automatically. Create feedback loops to then bring the outcomes of the Threat Hunt into detection content

1.3.11 **Service Threat Reporting** - as defined within section 5 of this Service Specific Schedule, create and deliver the required service reports and service review meetings to be able to validate to the Customer that the service is being delivered in the way in which it should be, and to allow for the opportunity for the Customer and the Supplier to feedback to each other.

2. CUSTOMER OBLIGATIONS

2.1 The Customer shall not store, distribute or transmit any material on its systems in respect of which managed services are provided by the Supplier that:

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

2.1.2 facilitates illegal activity;

2.1.3 depicts sexually explicit images and/or

2.1.4 promotes unlawful violence, discrimination based on race, gender, age, disability, sexual orientation, religion, belief or gender reassignment, or any other illegal activity.

3. SUPPORT TICKETS AND SERVICE LEVELS AGREEMENTS

3.1 The Customer may log any issues with the Supplier by telephone, email or web-portal ("Support Ticket") which shall be dealt with by the Supplier in accordance with the service levels identified in the table below.

3.2 Events or Alerts that the Service generates will, through consultation of the operational handbook and the Suppliers best industry knowledge, will be graded into the SLA service levels below.

3.2 The response and escalation times are dependent on the severity level of the Support Ticket as set out in the table below. Upon logging a Support Ticket with the Supplier's Support Engineer, an initial assessment shall be undertaken by the Supplier and a severity level discussed and agreed. The Customer should retain a record of any Support Ticket number which may be provided by the Support Engineer.

SEP 2

TECH DRIVEN.
PEOPLE POWERED.

SERVICE LEVEL	DESCRIPTION	HOURS OF COVER	RESPONSE TIME	SEP2 INTERNAL ESCALATION ROUTE	ESCALATION PATHWAY TO CUSTOMER (Only for Standard and Enhanced levels)
1	**Platform / Service Impact** System Down. Production service or other mission-critical system(s) are down and no workaround is immediately available. This will impact all users **Defined / Understood Security Incidents** High confidence/severity threat that if confirmed and uncontained is likely to have a significant impact to the Confidentiality, Integrity or Availability of one or more of the customer's production systems. **24/7 Analyst Led Awareness / Areas of Interest** Repeated instances of potentially related but disparate security detections have occurred that warrant a severity 1 response and further analysis	7 days a week 24 hours a day 24 x 7	SEP2 SOC team consolidate and verify event information and provide initial analysis within 15 minutes of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 SecOps Specialist or NetSec team if further technical input or analysis is required or if the original issue is outstanding after 30 minutes. SEP2 NetSec team escalates to Vendor Support in cases of Platform issues.	In cases triaged and identified as False Positive, notification / escalation is not performed but is included in service reporting / dashboards for visibility. Active / ongoing Severity 1 issues notified to customer either at pre-determined point in agreed playbook or as needed on the basis of SEP2 requiring the customer to take remedial/preventative/further actions themselves, or to provide further additional business context that may be required.
2	**Platform / Service Impact** System is operating a degraded service to	7 days a week	SEP2 SOC consolidate and	SEP2 SOC escalate to SEP2 SecOps Specialist	In cases triaged and identified as False Positive, notification /

	all users. One of more subsystems are not functioning or are impacting only a subset of users. **Defined / Understood Security Incidents** Medium confidence/severity threat that if confirmed and uncontained could impact the Confidentiality, Integrity or Availability of one or more of the customer's production systems. **24/7 Analyst Led Awareness / Areas of Interest** Repeated instances of potentially related but disparate security detections have occurred that warrant a severity 2 response and further analysis.	24 hours a day 24 x 7	verify event information and provide initial analysis within 1 hour of initial report and begin further investigations or remedial actions as soon as technically able.	or NetSec team if further technical input or analysis is required or if the original issue is outstanding after 60 minutes. SEP2 NetSec team escalates to Vendor Support in cases of Platform issues.	escalation is not performed but is included in service reporting / dashboards for visibility. Active / ongoing Severity 2 issues notified to customer either at pre-determined point in agreed playbook or as needed on the basis of SEP2 requiring the customer to take remedial/preventative/further actions themselves, or to provide further additional business context that may be required.
3	**Platform / Service Impact** All major functionality is working. Non-critical system issues. Impaired operations of some components but allows the user to continue using the system. **Defined / Understood Security Incidents** A low confidence action, that under many scenarios will be non-malicious and	7 days a week 24 hours a day 24 x 7	SEP2 SOC consolidate and verify event information and provide initial analysis within 4 hours of initial report and begin further investigations or	SEP2 SOC escalate to SEP2 SecOps Specialist or NetSec team if further technical input or analysis is required or if the original issue is outstanding after 8 hours. SEP2 NetSec team escalates to Vendor	In cases triaged and identified as False Positive, notification / escalation is not performed but is included in service reporting / dashboards for visibility. Active / ongoing Severity 3 issues notified to customer either at pre-determined point in agreed playbook or as

	requires additional context to verify if malicious intent has occurred.		remedial actions as soon as technically able.	Support in cases of Platform issues.	needed on the basis of SEP2 requiring the customer to take remedial/preventative/further actions themselves, or to provide further additional business context that may be required.
4	**Platform / Service Impact** General enquiries. No service degradation. **Defined / Understood Security Incidents** A high volume alert that is a known false positive, that poses little or no security risk and that has not yet been remediated or tuned.	7 days a week 24 hours a day 24 x 7	SEP2 SOC consolidate and verify event information and provide initial analysis within 8 hours of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 SecOps Specialist or NetSec team if further technical input or analysis is required or if the original issue is outstanding after 24 hours.	No escalation of this severity of issue to the customer is performed, but statistics and information on these events are included in reporting and are available in the SOAR dashboards.

4. SERVICE DEPLOYMENT

4.1 A planning session will be held between the Supplier and the Customer where specific requirements are captured and a working implementation plan is developed and agreed upon, as well as mutual agreement by both the Supplier and Customer as to timelines, milestones, and key dates to achieve transition to “live”. Neither party shall be unreasonable in providing agreement and sufficient resources to ensure that the timelines agreed are achievable.

4.2 The Supplier makes use of a project management tool, Halo, which it will allow the Customer access to, to be able to track and manage the process of the implementation. Exports from Halo can be taken via CSV/Excel as needed should the Customer need to manage data in their own environment.
4.2.1 The Supplier may use alternative specific tools from time to time at their discretion, so long as suitability of tools is largely inline with the functions that Halo provide.

4.2.2 After the planning and scoping session, the specific agreed tasks and milestones, capturing resourcing requirements from both the Supplier and the Customer will be added into the Halo project.

4.3 The Customer will ensure that they make available to the Supplier suitably experienced and authorised personnel to be able to facilitate the service implementation, considering required authentication and access to log sources and ability to enact changes as needed to facilitate log source onboarding.

4.4 During the service implementation phase, and subject to mutual agreement to change the frequency, a weekly update meeting will be held. The scope of that meeting is from a project management perspective, to ensure that the deployment is being completed as per the agreed plan created within the planning and scoping session.

4.4.1 Should any issues, dependencies, problems or other such be identified within this meeting, the respective party (either the Customer or the Supplier) will endeavor to provide further details and plans on how that can be remediated.
4.4.2 At a point which is mutually agreed upon by both the Supplier and the Customer, this scheduled update meeting can be stopped, at which point the service is deemed to have been deployed to live stage, and the service has entered into the business as usual phase.

4.5 During the implementation phase and thereafter as needed, the Supplier and the Customer will make use of the best possible methods of shared and communal communication, such as a shared Teams, Slack or Google Chat channel.

5. REPORTING & BUSINESS CONTINUITY

5.1 For customers of the Wingman EDR Enhanced level only, the Supplier shall provide reports to the Customer which summarises the Services provided to the Customer in the previous 90 days, on a rolling 90 day basis. Notwithstanding the foregoing, the Supplier and Customer shall have Service review meetings at a location to be mutually agreed on a rolling 90 day basis. The Service review meetings shall be attended by key contacts of both the Supplier and Customer to be mutually agreed in advance. The purpose of the Service review meetings is to allow either party to provide feedback on the Services.
5.2 The Supplier shall implement a disaster recovery plan which sets out the Supplier's approach to ensure business continuity for the Services. The Supplier shall regularly carry out testing of its procedures for this purpose

6. SERVICE HANDOVER / EXIT TRANSITION

6.1 Irrespective of the methodology or reasons why a Termination (Clause 9 of the Terms and Conditions) has occurred, or in the case where the Contract is in its final month and is not intended to be extended/renewed by the Customer, the Supplier warrants that it shall act reasonably and with good faith to help and facilitate the Customer in the actions which may be required to support the Customer in moving to an alternative provider or platform.

7. THIRD PARTY SOFTWARE

7.1 Where the Wingman MDR quotation lists Crowdstrike as the EDR technology included, the Crowdstrike Terms and Conditions available at https://www.crowdstrike.com/en-us/legal/terms-conditions/ fall within the scope of the EULA.
7.2 Where the Wingman MDR quotation lists SentinelOne as the EDR technology included, the Sentinel One Terms and Conditions fall within the scope of the EULA and are available at https://www.sentinelone.com/legal/, where the relevant sections are included:

- "Customer > Master Subscription Agreement"
- "Customer > Solutions Addendum: Singularity Platform Terms"
- "Customer > Support Terms"
- "Privacy > Privacy Notice"

- “Privacy > Data Protection Addendum”
- “Privacy > List of Sub-processors”
- “Intellectual Property > Patents”

TECH DRIVEN.
PEOPLE POWERED.

SERVICE-SPECIFIC SCHEDULE: MANAGED SERVICES ("Wingman Secure Access")

Where the Supplier provides a 'managed service' to the Customer, the following terms shall apply.

1. PROVISION OF MANAGED SERVICES

1.1 The Supplier shall provide managed services only in respect of the goods/software/equipment supplied by the Supplier (or as otherwise expressly identified in the Quotation).

1.2 The Supplier does not warrant that the Supplier's provision of, and the Customer's use of, the managed services will be uninterrupted or error-free.

Wingman Secure Access Basic Includes:
1.3 **Deployment of the Service**, in accordance with section 4 of this Service Specific Schedule
1.3.1 **Unlimited Guided Support** - Complete relevant and appropriate troubleshooting with the Customer and the Customer users to resolve problems identified, aligned to the SLA table as provided below in section 3 of this Service Specific Schedule
1.3.2 **Vendor Issue Escalation** - In cases where troubleshooting and policy management cannot resolve an issue, the Supplier will escalate to the Vendor for Vendor support as required.
1.3.3 **Vendor Product Alerts** - The Supplier will issue to the Customer updates and alerts that the vendor makes available, for the Customers awareness.

Wingman Secure Access Standard Includes:
1.3.4 **Initial Health Check** - Provides for a Health Check of the estate within the scope of the service to find any specific issues that should be addressed.
1.3.5 **Unlimited Change Requests -** to ensure that the Service is adapting to the Customers changing environment, the Supplier shall use best endeavours to comply with day-to-day changes to the Customer's environment as requested by the Customer's employees ("Change Requests") in accordance with the target

response times in the table below provided always that such Change Requests are limited to the features of the relevant equipment and service supplied by the Supplier, and the Supplier has sufficient resources available to comply with such Change Requests. In the table below, “Action” means that an engineer will review the change request and either complete the change as requested or respond to the requestor of the change seeking further information necessary to complete the change.

PRIORITY	DESCRIPTION	RESPONSE TIME (FOR RECEIPT OF CHANGE REQUEST)
1. Urgent	Change required in order to provide a workaround for a critical issue	Action within 2 hours
2. Unplanned	Ad-Hoc change that is not part of a pre-defined project	Action within 8 working hours
3. Planned	Change as part of a pre-defined project	Action within 24 working hours

1.3.6 **Device Monitoring -** The Supplier shall use reasonable endeavours to monitor the relevant equipment on a 24x7x365 basis using a dedicated monitoring platform. The Supplier shall monitor the following key metrics and any abnormal results shall result in a support ticket being raised with the Supplier (in which case the support ticket shall be dealt with in accordance with the terms of the SLA table as per section 3 of this Service Specific Schedule): CPU utilisation; vendor-specific process information; available disk space; RAM and swap memory utilisation; system uptime; and interface status and throughput

1.3.7 **Device Backups** - The Supplier shall carry out weekly configuration backups of supported equipment within the scope of the service as defined within the Quotation capable of being backed up to ensure that there is an available and sufficient configuration of such equipment to restore in the case of a catastrophic failure of some or all of such equipment, or where there is a problematic configuration change which needs to be reverted to a workable version. Where the backups have failed, this shall result in a support ticket being raised with the Supplier (in which case the support ticket shall be dealt with in accordance with the terms of the SLA table as per section 3 of this Service Specific Schedule)

1.3.8 **Security Patching** - The Supplier may from time to time (and where the Supplier considers it necessary) complete version upgrades and patch the

relevant equipment as a result of any software bug or security vulnerability. Where upgrades and/or patching is required, the Supplier shall agree a mutual data and time for this to occur. For the avoidance of doubt, the update shall be carried out remotely from the Supplier's registered office (or any other location notified by the Supplier). The Customer may request to have on-site Supplier personnel to carry out the update, but this will be subject to additional charges which are to be agreed in writing. The Customer acknowledges and agrees that the Supplier shall only be able to comply with this paragraph 1.3.8 where such upgrade or patching is made available by a third party vendor and the Supplier shall have no liability to the Customer where no such upgrade or patch is available.

1.3.9 **Annual Major Version Upgrades** - The Supplier shall, on an annual basis perform an update to the most recent software or firmware version to the relevant equipment at a time and date mutually agreed with the Customer. For the avoidance of doubt, the update shall be carried out remotely from the Supplier's registered office (or any other location notified by the Supplier). The Customer may request to have on-site Supplier personnel to carry out the update, but this will be subject to additional charges which are to be agreed in writing. The Customer acknowledges and agrees that the Supplier shall only be able to comply with this paragraph 1.3.9 where such update is made available by a third party vendor and the Supplier shall have no liability to the Customer where no such update is available.

1.3.10 **Rolling Recommended Patching** - The Supplier may from time to time (and where the Supplier considers it necessary) complete version upgrades and patch the relevant equipment to the latest available "recommended" software release available from the applicable third party vendor. Where upgrades and/or patching is required, the Supplier shall agree a mutual data and time for this to occur. For the avoidance of doubt, the update shall be carried out remotely from the Supplier's registered office (or any other location notified by the Supplier). The Customer may request to have on-site Supplier personnel to carry out the update, but this will be subject to additional charges which are to be agreed in writing. The Customer acknowledges and agrees that the Supplier shall only be able to comply with this paragraph 1.3.8 where such upgrade or patching is made available by a third party vendor and the Supplier shall have no liability to the Customer where no such upgrade or patch is available.

<u>Wingman Secure Access Enhanced Includes:</u>

1.3.11 **Rolling Proactive Policy Reviews** - The supplier will provide proactive and ongoing Policy Reviews, delivered through a support ticket to the Customer on an ongoing basis.

1.3.12 **Rolling Proactive Health Checks** - The supplier will provide proactive and ongoing Health Checks, delivered through a support ticket to the Customer on an ongoing basis.

2. CUSTOMER OBLIGATIONS

2.1 The Customer shall not store, distribute or transmit any material on its systems in respect of which managed services are provided by the Supplier that:
2.1.1 is unlawful, harmful, threatening, defamatory, obscene, harassing or racially or ethnically offensive;
2.1.2 facilitates illegal activity;
2.1.3 depicts sexually explicit images and/or
2.1.4 promotes unlawful violence, discrimination based on race, gender, age, disability, sexual orientation, religion, belief or gender reassignment, or any other illegal activity.

3. SUPPORT TICKETS AND SERVICE LEVELS AGREEMENTS

3.1 The Customer may log any issues with the Supplier by telephone, email or web-portal ("Support Ticket") which shall be dealt with by the Supplier in accordance with the service levels identified in the table below.

3.2 Events or Alerts that the Service generates will, through consultation of the operational handbook and the Suppliers best industry knowledge, will be graded into the SLA service levels below.

3.2 The response and escalation times are dependent on the severity level of the Support Ticket as set out in the table below. Upon logging a Support Ticket with the Supplier's Support Engineer, an initial assessment shall be undertaken by the Supplier and a severity level discussed and agreed. The Customer should retain a record of any Support Ticket number which may be provided by the Support Engineer.

SEP 2

TECH DRIVEN.
PEOPLE POWERED.

SERVICE LEVEL	DESCRIPTION	HOURS OF COVER	RESPONSE TIME	SEP2 INTERNAL ESCALATION ROUTE
1	**Platform / Service Impact** System Down. Production service or other mission-critical system(s) are down and no workaround is immediately available. This will impact all users	7 days a week 24 hours a day 24 x 7	SEP2 SOC team consolidate and verify event information and provide initial analysis within 15 minutes of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 NetSec team if further technical input or analysis is required or if the original issue is outstanding after 30 minutes. SEP2 NetSec team escalates to Vendor Support in cases of Platform issues.
2	**Platform / Service Impact** System is operating a degraded service to all users. One of more subsystems are not functioning or are impacting only a subset of users.	7 days a week 24 hours a day 24 x 7	SEP2 SOC team consolidate and verify event information and provide initial analysis within 1 hour of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 NetSec team if further technical input or analysis is required or if the original issue is outstanding after 60 minutes. SEP2 NetSec team escalates to Vendor Support in cases of Platform issues.
3	**Platform / Service Impact** All major functionality is working. Non-critical	7 days a week 24 hours a day 24 x 7	SEP2 SOC team consolidate and verify event information and	SEP2 SOC escalate to SEP2 NetSec team if further technical input or analysis

	system issues. Impaired operations of some components but allows the user to continue using the system.		provide initial analysis within 4 hours of initial report and begin further investigations or remedial actions as soon as technically able.	is required or if the original issue is outstanding after 8 hours. SEP2 NetSec team escalates to Vendor Support in cases of Platform issues.
4	**Platform / Service Impact** General enquiries. No service degradation.	7 days a week 24 hours a day 24 x 7	SEP2 SOC consolidate and verify event information and provide initial analysis within 8 hours of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 NetSec team if further technical input or analysis is required or if the original issue is outstanding after 24 hours.

4. SERVICE DEPLOYMENT

4.1 A planning session will be held between the Supplier and the Customer where specific requirements are captured and a working implementation plan is developed and agreed upon, as well as mutual agreement by both the Supplier and Customer as to timelines, milestones, and key dates to achieve transition to “live”. Neither party shall be unreasonable in providing agreement and sufficient resources to ensure that the timelines agreed are achievable.

4.2 The Supplier makes use of a project management tool, Halo, which it will allow the Customer access to, to be able to track and manage the process of the implementation. Exports from Halo can be taken via CSV/Excel as needed should the Customer need to manage data in their own environment.
4.2.1 The Supplier may use alternative specific tools from time to time at their discretion, so long as suitability of tools is largely inline with the functions that Halo provide.

4.2.2 After the planning and scoping session, the specific agreed tasks and milestones, capturing resourcing requirements from both the Supplier and the Customer will be added into the Halo project.

4.3 The Customer will ensure that they make available to the Supplier suitably experienced and authorised personnel to be able to facilitate the service implementation, considering required authentication and access to log sources and ability to enact changes as needed to facilitate log source onboarding.

4.4 During the service implementation phase, and subject to mutual agreement to change the frequency, a weekly update meeting will be held. The scope of that meeting is from a project management perspective, to ensure that the deployment is being completed as per the agreed plan created within the planning and scoping session.

4.4.1 Should any issues, dependencies, problems or other such be identified within this meeting, the respective party (either the Customer or the Supplier) will endeavor to provide further details and plans on how that can be remediated.
4.4.2 At a point which is mutually agreed upon by both the Supplier and the Customer, this scheduled update meeting can be stopped, at which point the service is deemed to have been deployed to live stage, and the service has entered into the business as usual phase.

4.5 During the implementation phase and thereafter as needed, the Supplier and the Customer will make use of the best possible methods of shared and communal communication, such as a shared Teams, Slack or Google Chat channel.

5. REPORTING & BUSINESS CONTINUITY

5.1 For customers of the Wingman Secure Access Standard and Enhanced levels only, the Supplier shall provide reports to the Customer which summarises the Services provided to the Customer in the previous 90 days, on a rolling 90 day basis. Notwithstanding the foregoing, the Supplier and Customer shall have Service review meetings at a location to be mutually agreed on a rolling 90 day basis. The Service review meetings shall be attended by key contacts of both the Supplier and Customer to be mutually agreed in advance. The purpose of the Service review meetings is to allow either party to provide feedback on the Services.
5.2 The Supplier shall implement a disaster recovery plan which sets out the Supplier's approach to ensure business continuity for the Services. The Supplier shall regularly carry out testing of its procedures for this purpose

6. SERVICE HANDOVER / EXIT TRANSITION

6.1 Irrespective of the methodology or reasons why a Termination (Clause 9 of the Terms and Conditions) has occurred, or in the case where the Contract is in its final month and is not intended to be extended/renewed by the Customer, the Supplier warrants that it shall act reasonably and with good faith to help and facilitate the Customer in the actions which may be required to support the Customer in moving to an alternative provider or platform.

TECH DRIVEN.
PEOPLE POWERED.

SERVICE-SPECIFIC SCHEDULE: MANAGED SERVICES ("Wingman Cloud")

Where the Supplier provides a 'managed service' to the Customer, the following terms shall apply.

1. PROVISION OF MANAGED SERVICES

1.1 The Supplier shall provide managed services only in respect of the goods/software/equipment supplied by the Supplier (or as otherwise expressly identified in the Quotation).

1.2 The Supplier does not warrant that the Supplier's provision of, and the Customer's use of, the managed services will be uninterrupted or error-free.

Wingman Cloud Basic Includes:
1.3 **Deployment of the Service**, in accordance with section 4 of this Service Specific Schedule
1.3.3 **Critical Risk Assessment** - Complete an assessment of the Critical Risks as discovered in the deployment phase to assist the Customer in addressing these risks.
1.3.4 **Knowledge Transfer Session** - A virtual session during which specifical knowledge, awareness and experience of the platform and its features is shared with the Customer to increase their operational knowledge of the platform and the service.
1.3.5 **Unlimited office hours support** – Aligned to the "Platform / Service Impact" component only of the SLA within clause 3 of this Service Specific Schedule, the Supplier will provide support and assistance to the Customer with no limits as to the amount of time delivered.
1.3.6 **Vendor Issue Escalation -** In cases where troubleshooting and policy management cannot resolve an issue, the Supplier will escalate to the Vendor for Vendor support as required.

Wingman Cloud Standards adds:
1.3.7 **Extended Onboarding Window -** Provides more flexibility and time for initial service onboarding to be completed.
1.3.8 **Unlimited Changes and Integrations** - to ensure that the Service is adapting to the Customers changing environment, the Supplier shall use best endeavours

to comply with day-to-day changes to the Customer's environment as requested by the Customer's employees ("Change Requests") in accordance with the target response times in the table below provided always that such Change Requests are limited to the features of the relevant equipment and service supplied by the Supplier, and the Supplier has sufficient resources available to comply with such Change Requests. In the table below, "Action" means that an engineer will review the change request and either complete the change as requested or respond to the requestor of the change seeking further information necessary to complete the change.

PRIORITY	DESCRIPTION	RESPONSE TIME (FOR RECEIPT OF CHANGE REQUEST)
1. Urgent	Change required in order to provide a workaround for a critical issue	Action within 2 hours
2. Unplanned	Ad-Hoc change that is not part of a pre-defined project	Action within 8 working hours
3. Planned	Change as part of a pre-defined project	Action within 24 working hours

1.3.9 **In-Depth Review of Findings and Remediation Advice** - Expand the scope of the Critical Risk Assessment to include all findings and provide remediation or recommendations to address the findings.
1.3.10 **Periodic Review of Cloud Estate Health** - The customer may schedule periodic Wingman sessions with the Supplier to provide for periodic reviews of the Cloud Estate Health as shown within the platform and to provide ongoing support and assistance in use and configuration.

<u>Wingman Cloud Enhanced adds:</u>
1.3.11 **24x7 Monitoring of Alerts via SEP2 SOC & Alert Triage and Response** - Aligned to the "Defined / Understood Security Incidents" and "24/7 Analyst Led Awareness / Areas of Interest" components of the SLA within clause 3 of this Service Specific Schedule, the Supplier will provide triage, investigation and escalation actions based on events detected.
1.3.12 **Access to SEP2 Cloud Architects** - The Customer will have access to Cloud Architect resources within the SEP2 Wingman Security Operations team to provide architectural advisory services as part of the contract.

2. CUSTOMER OBLIGATIONS

2.1 The Customer shall not store, distribute or transmit any material on its systems in respect of which managed services are provided by the Supplier that:
2.1.1 is unlawful, harmful, threatening, defamatory, obscene, harassing or racially or ethnically offensive;
2.1.2 facilitates illegal activity;
2.1.3 depicts sexually explicit images and/or
2.1.4 promotes unlawful violence, discrimination based on race, gender, age, disability, sexual orientation, religion, belief or gender reassignment, or any other illegal activity.

3. SUPPORT TICKETS AND SERVICE LEVELS AGREEMENTS

3.1 The Customer may log any issues with the Supplier by telephone, email or web-portal ("Support Ticket") which shall be dealt with by the Supplier in accordance with the service levels identified in the table below.

3.2 Events or Alerts that the Service generates will, through consultation of the operational handbook and the Suppliers best industry knowledge, will be graded into the SLA service levels below.

3.2 The response and escalation times are dependent on the severity level of the Support Ticket as set out in the table below. Upon logging a Support Ticket with the Supplier's Support Engineer, an initial assessment shall be undertaken by the Supplier and a severity level discussed and agreed. The Customer should retain a record of any Support Ticket number which may be provided by the Support Engineer.

SEP 2

TECH DRIVEN.
PEOPLE POWERED.

SERVICE LEVEL	DESCRIPTION	HOURS OF COVER	RESPONSE TIME	SEP2 INTERNAL ESCALATION ROUTE
1	**Platform / Service Impact** System Down. Production service or other mission-critical system(s) are down and no workaround is immediately available. This will impact all users **Defined / Understood Security Incidents** High confidence/severity threat that if confirmed and uncontained is likely to have a significant impact to the Confidentiality, Integrity or Availability of one or more of the customer's production systems. **24/7 Analyst Led Awareness / Areas of Interest** Repeated instances of potentially related but disparate security detections have occurred that warrant a severity 1 response and further analysis	7 days a week 24 hours a day 24 x 7	SEP2 SOC team consolidate and verify event information and provide initial analysis within 15 minutes of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 NetSec team if further technical input or analysis is required or if the original issue is outstanding after 30 minutes. SEP2 NetSec team escalates to Vendor Support in cases of Platform issues.
2	**Platform / Service Impact** System is operating a degraded service to	7 days a week 24 hours a day	SEP2 SOC consolidate and	SEP2 SOC escalate to SEP2 NetSec team if further

	all users. One of more subsystems are not functioning or are impacting only a subset of users. **Defined / Understood Security Incidents** Medium confidence/severity threat that if confirmed and uncontained could impact the Confidentiality, Integrity or Availability of one or more of the customer's production systems. **24/7 Analyst Led Awareness / Areas of Interest** Repeated instances of potentially related but disparate security detections have occurred that warrant a severity 2 response and further analysis.	24 x 7	verify event information and provide initial analysis within 1 hour of initial report and begin further investigations or remedial actions as soon as technically able.	technical input or analysis is required or if the original issue is outstanding after 60 minutes. SEP2 NetSec team escalates to Vendor Support in cases of Platform issues.
3	**Platform / Service Impact** All major functionality is working. Non-critical system issues. Impaired operations of some components but allows the user to continue using the system. **Defined / Understood Security Incidents**	7 days a week 24 hours a day 24 x 7	SEP2 SOC consolidate and verify event information and provide initial analysis within 4 hours of initial report and begin further	SEP2 SOC escalate to SEP2 NetSec team if further technical input or analysis is required or if the original issue is outstanding after 8 hours. SEP2 NetSec team escalates to Vendor Support in cases of

	A low confidence action, that under many scenarios will be non-malicious and requires additional context to verify if malicious intent has occurred.		investigations or remedial actions as soon as technically able.	Platform issues.
4	**Platform / Service Impact** General enquiries. No service degradation. **Defined / Understood Security Incidents** A high volume alert that is a known false positive, that poses little or no security risk and that has not yet been remediated or tuned.	7 days a week 24 hours a day 24 x 7	SEP2 SOC consolidate and verify event information and provide initial analysis within 12 hours of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 NetSec team if further technical input or analysis is required or if the original issue is outstanding after 24 hours.

4. SERVICE DEPLOYMENT

4.1 A planning session will be held between the Supplier and the Customer where specific requirements are captured and a working implementation plan is developed and agreed upon, as well as mutual agreement by both the Supplier and Customer as to timelines, milestones, and key dates to achieve transition to “live”. Neither party shall be unreasonable in providing agreement and sufficient resources to ensure that the timelines agreed are achievable.

4.2 The Supplier makes use of a project management tool, Halo, which it will allow the Customer access to, to be able to track and manage the process of the implementation. Exports from Halo can be taken via CSV/Excel as needed should the Customer need to manage data in their own environment.
4.2.1 The Supplier may use alternative specific tools from time to time at their discretion, so long as suitability of tools is largely inline with the functions that Halo provide.

4.2.2 After the planning and scoping session, the specific agreed tasks and milestones, capturing resourcing requirements from both the Supplier and the Customer will be added into the Halo project.

4.3 The Customer will ensure that they make available to the Supplier suitably experienced and authorised personnel to be able to facilitate the service implementation, considering required authentication and access to log sources and ability to enact changes as needed to facilitate log source onboarding.

4.4 During the service implementation phase, and subject to mutual agreement to change the frequency, a weekly update meeting will be held. The scope of that meeting is from a project management perspective, to ensure that the deployment is being completed as per the agreed plan created within the planning and scoping session.

4.4.1 Should any issues, dependencies, problems or other such be identified within this meeting, the respective party (either the Customer or the Supplier) will endeavor to provide further details and plans on how that can be remediated.
4.4.2 At a point which is mutually agreed upon by both the Supplier and the Customer, this scheduled update meeting can be stopped, at which point the service is deemed to have been deployed to live stage, and the service has entered into the business as usual phase.

4.5 During the implementation phase and thereafter as needed, the Supplier and the Customer will make use of the best possible methods of shared and communal communication, such as a shared Teams, Slack or Google Chat channel.

5. REPORTING & BUSINESS CONTINUITY

5.1 For customers of the Wingman Cloud Enhanced level only, the Supplier shall provide reports to the Customer which summarises the Services provided to the Customer in the previous 90 days, on a rolling 90 day basis. Notwithstanding the foregoing, the Supplier and Customer shall have Service review meetings at a location to be mutually agreed on a rolling 90 day basis. The Service review meetings shall be attended by key contacts of both the Supplier and Customer to be mutually agreed in advance. The purpose of the Service review meetings is to allow either party to provide feedback on the Services.
5.2 The Supplier shall implement a disaster recovery plan which sets out the Supplier's approach to ensure business continuity for the Services. The Supplier shall regularly carry out testing of its procedures for this purpose

6. SERVICE HANDOVER / EXIT TRANSITION

6.1 Irrespective of the methodology or reasons why a Termination (Clause 9 of the Terms and Conditions) has occurred, or in the case where the Contract is in its final month and is not intended to be extended/renewed by the Customer, the Supplier warrants that it shall act reasonably and with good faith to help and facilitate the Customer in the actions which may be required to support the Customer in moving to an alternative provider or platform.

7. THIRD PARTY SOFTWARE

7.1 Wiz Terms and Conditions (https://legal.wiz.io/legal) are within the scope of these terms within the EULA.

TECH DRIVEN.
PEOPLE POWERED.

SERVICE-SPECIFIC SCHEDULE: MANAGED SERVICES ("Wingman Human Risk")

Where the Supplier provides a 'managed service' to the Customer, the following terms shall apply.

1. PROVISION OF MANAGED SERVICES

1.1 The Supplier shall provide managed services only in respect of the goods/software/equipment supplied by the Supplier (or as otherwise expressly identified in the Quotation).

1.2 The Supplier does not warrant that the Supplier's provision of, and the Customer's use of, the managed services will be uninterrupted or error-free.

Wingman Human Risk - Email Basic Includes:
1.3 **Deployment of the Service**, in accordance with section 4 of this Service Specific Schedule
1.3.1 **Email based Support - 10 Requests -** Support delivered in alignment with the SLA in section 3 of this Service Specific Schedule, limited to 10 interactions / tickets within your contract.

Wingman Human Risk - Email Standard adds:
1.3.2 **Email based Support - Unlimited Requests** - Upgrades to unlimited number of Support interactions within your contract, delivered via email, aligned to the SLA in section 3 of this Service Specific Schedule

Wingman Human Risk - Email Enhanced adds:
1.3.3 **Email, Phone and Teams or Zoom based support, unlimited requests** - Allows for support interactions via the mentioned platforms in addition to email.

Wingman Human Risk - Security Awareness Basic Includes:
1.4 **Deployment of the Service**, in accordance with section 4 of this Service Specific Schedule
1.4.1 **Email based Support - 10 Requests -** Support delivered in alignment with the SLA in section 3 of this Service Specific Schedule, limited to 10 interactions / tickets within your contract.

Wingman Human Risk - Security Awareness Standard Includes:
1.4.2 **Email based Support - Unlimited Requests** - Upgrades to unlimited number of Support interactions within your contract, delivered via email, aligned to the SLA in section 3 of this Service Specific Schedule

Wingman Human Risk - Security Awareness Enhanced adds:
1.4.3 **Email, Phone and Teams or Zoom based support, unlimited requests** - Allows for support interactions via the mentioned platforms in addition to email.

2. CUSTOMER OBLIGATIONS

2.1 The Customer shall not store, distribute or transmit any material on its systems in respect of which managed services are provided by the Supplier that:
2.1.1 is unlawful, harmful, threatening, defamatory, obscene, harassing or racially or ethnically offensive;
2.1.2 facilitates illegal activity;
2.1.3 depicts sexually explicit images and/or
2.1.4 promotes unlawful violence, discrimination based on race, gender, age, disability, sexual orientation, religion, belief or gender reassignment, or any other illegal activity.

3. SUPPORT TICKETS AND SERVICE LEVELS AGREEMENTS

3.1 The Customer may log any issues with the Supplier by telephone, email or web-portal (“Support Ticket”) which shall be dealt with by the Supplier in accordance with the service levels identified in the table below.

3.2 Events or Alerts that the Service generates will, through consultation of the operational handbook and the Suppliers best industry knowledge, will be graded into the SLA service levels below.

3.2 The response and escalation times are dependent on the severity level of the Support Ticket as set out in the table below. Upon logging a Support Ticket with the Supplier’s Support Engineer, an initial assessment shall be undertaken by the Supplier and a severity level discussed and agreed. The Customer should retain a record of any Support Ticket number which may be provided by the Support Engineer.

SEP 2

TECH DRIVEN.
PEOPLE POWERED.

SERVICE LEVEL	DESCRIPTION	HOURS OF COVER	RESPONSE TIME	SEP2 INTERNAL ESCALATION ROUTE
1	**Platform / Service Impact** System Down. Production service or other mission-critical system(s) are down and no workaround is immediately available. This will impact all users	7 days a week 24 hours a day 24 x 7	SEP2 SOC team consolidate and verify event information and provide initial analysis within 15 minutes of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 NetSec team if further technical input or analysis is required or if the original issue is outstanding after 30 minutes. SEP2 NetSec team escalates to Vendor Support in cases of Platform issues.
2	**Platform / Service Impact** System is operating a degraded service to all users. One of more subsystems are not functioning or are impacting only a subset of users.	7 days a week 24 hours a day 24 x 7	SEP2 SOC team consolidate and verify event information and provide initial analysis within 1 hour of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 NetSec team if further technical input or analysis is required or if the original issue is outstanding after 60 minutes. SEP2 NetSec team escalates to Vendor Support in cases of Platform issues.
3	**Platform / Service Impact** All major functionality is working. Non-critical	7 days a week 24 hours a day 24 x 7	SEP2 SOC team consolidate and verify event information and	SEP2 SOC escalate to SEP2 NetSec team if further technical input or analysis

	system issues. Impaired operations of some components but allows the user to continue using the system.		provide initial analysis within 4 hours of initial report and begin further investigations or remedial actions as soon as technically able.	is required or if the original issue is outstanding after 8 hours. SEP2 NetSec team escalates to Vendor Support in cases of Platform issues.
4	**Platform / Service Impact** General enquiries. No service degradation.	7 days a week 24 hours a day 24 x 7	SEP2 SOC consolidate and verify event information and provide initial analysis within 8 hours of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 NetSec team if further technical input or analysis is required or if the original issue is outstanding after 24 hours.

4. SERVICE DEPLOYMENT

4.1 A planning session will be held between the Supplier and the Customer where specific requirements are captured and a working implementation plan is developed and agreed upon, as well as mutual agreement by both the Supplier and Customer as to timelines, milestones, and key dates to achieve transition to “live”. Neither party shall be unreasonable in providing agreement and sufficient resources to ensure that the timelines agreed are achievable.

4.2 The Supplier makes use of a project management tool, Halo, which it will allow the Customer access to, to be able to track and manage the process of the implementation. Exports from Halo can be taken via CSV/Excel as needed should the Customer need to manage data in their own environment.
4.2.1 The Supplier may use alternative specific tools from time to time at their discretion, so long as suitability of tools is largely inline with the functions that Halo provide.

4.2.2 After the planning and scoping session, the specific agreed tasks and milestones, capturing resourcing requirements from both the Supplier and the Customer will be added into the Halo project.

4.3 The Customer will ensure that they make available to the Supplier suitably experienced and authorised personnel to be able to facilitate the service implementation, considering required authentication and access to log sources and ability to enact changes as needed to facilitate log source onboarding.

4.4 During the service implementation phase, and subject to mutual agreement to change the frequency, a weekly update meeting will be held. The scope of that meeting is from a project management perspective, to ensure that the deployment is being completed as per the agreed plan created within the planning and scoping session.

4.4.1 Should any issues, dependencies, problems or other such be identified within this meeting, the respective party (either the Customer or the Supplier) will endeavor to provide further details and plans on how that can be remediated.
4.4.2 At a point which is mutually agreed upon by both the Supplier and the Customer, this scheduled update meeting can be stopped, at which point the service is deemed to have been deployed to live stage, and the service has entered into the business as usual phase.

4.5 During the implementation phase and thereafter as needed, the Supplier and the Customer will make use of the best possible methods of shared and communal communication, such as a shared Teams, Slack or Google Chat channel.

5. BUSINESS CONTINUITY

5.1 The Supplier shall implement a disaster recovery plan which sets out the Supplier's approach to ensure business continuity for the Services. The Supplier shall regularly carry out testing of its procedures for this purpose

6. SERVICE HANDOVER / EXIT TRANSITION

6.1 Irrespective of the methodology or reasons why a Termination (Clause 9 of the Terms and Conditions) has occurred, or in the case where the Contract is in its final month and is not intended to be extended/renewed by the Customer, the Supplier warrants that it shall act reasonably and with good faith to help and facilitate the Customer in the actions which may be required to support the Customer in moving to an alternative provider or platform.

7. THIRD PARTY SOFTWARE

7.1 Where the Wingman Human Risk quotation includes Human Risk Email, the Check Point Terms and Conditions available at https://www.checkpoint.com/about-us/cloud-terms/ fall within the scope of the EULA.
7.2 Where the Wingman Human Risk quotation includes User Awareness Training, the KnowBe4 Terms and Conditions available at https://www.knowbe4.com/legal/terms fall within the scope of the EULA.

TECH DRIVEN.
PEOPLE POWERED.

SERVICE-SPECIFIC SCHEDULE: MANAGED SERVICES ("Wingman GRC")

Where the Supplier provides a 'managed service' to the Customer, the following terms shall apply.

1. PROVISION OF MANAGED SERVICES

1.1 The Supplier shall provide managed governance, risk, and compliance services in respect of the scope identified in the Quotation. The Supplier does not warrant that the provision of these services will guarantee immunity from regulatory fines, legal action, or cyber-attacks

1.1 The Supplier shall provide managed services only in respect of the goods/software/equipment supplied by the Supplier (or as otherwise expressly identified in the Quotation).

1.2 The Supplier does not warrant that the Supplier's provision of, and the Customer's use of, the managed services will be uninterrupted or error-free.

1.3 Scope of Services:
1.3.1 **Dedicated Strategy Manager (vCISO)** - The Supplier shall provide a Dedicated Strategy Manager to act as a Board Level Executive Representative. This role includes providing expert analysis to ensure cyber security is at the forefront of planning, translating technical risk into business language, and justifying cyber security investments.
1.3.2 **Organisational Cyber Security Risk Strategy** - The Supplier will provide in-depth expert guidance to navigate the Customer's current posture and plan for future requirements. This includes the provision of ad-hoc Gap Analysis reports and strategic roadmaps.
1.3.3 **Compliance & Framework Audit Readiness** - The Supplier shall assist the Customer in achieving audit readiness for frameworks specified in the Quotation (e.g., ISO27001, NIST, DORA, PCI-DSS, Cyber Essentials Plus). The Supplier provides automation through tooling to facilitate data gathering.
The Supplier provides readiness support and advice; the Supplier does not act as the external auditor or certification body and cannot guarantee certification.
1.3.4 **Vendor Agnostic Advice -** The Supplier shall provide vendor-agnostic consultation to enable the greatest ROI on the Customer's investments.

1.3.5 **Vulnerability Detection and Patch Management** - If specified in the Quotation, the Supplier shall utilise automated workflows to detect vulnerabilities and facilitate patch management to keep critical asset patching up to date.
1.3.6 **Asset Management** - The Supplier shall utilise tooling to discover, classify, and manage known and unknown network assets to proactively manage exploits.

1.4 **Tooling** - The Wingman GRC service may utilise third-party platforms (such as Drata and Qualys) to power the service. The Supplier facilitates support for these platforms in either a co-managed or consultancy support role. If these tools are to be used by the Customer then they must be included within the Quotation of this service.

2. CUSTOMER OBLIGATIONS

2.1 **Implementation of Advice** - The Customer acknowledges that the Supplier provides advice, recommendations, and risk analysis. The Customer retains ultimate responsibility for accepting risk and deciding whether to implement the Supplier's recommendations. The Supplier shall not be liable for damages resulting from the Customer's failure to implement recommended remediation or security controls.
2.2 **Access and Authority** - The Customer must provide the Supplier with:
2.2.1 Sufficient access to stakeholders, including board-level personnel, to allow the Dedicated Strategy Manager to perform their duties.
2.2.2 Authorization to perform vulnerability scans and asset discovery on the Customer's network. The Customer warrants they have the right to authorise scans on all targeted IP addresses.
2.3 **Audit Evidence** - The Customer is responsible for providing accurate and timely evidence, documentation, and data required for compliance frameworks. The Supplier is not responsible for delays caused by the Customer's failure to provide necessary compliance data

3. SUPPORT TICKETS AND SERVICE LEVELS AGREEMENTS

3.1 The Customer may log any issues with the Supplier by telephone, email or web-portal ("Support Ticket") which shall be dealt with by the Supplier in accordance with the service levels identified in the table below.

3.2 Events or Alerts that the Service generates will, through consultation of the operational handbook and the Suppliers best industry knowledge, will be graded into the SLA service levels below.

3.3 The Customer may log issues regarding the GRC platform (e.g, Drata, Qualys) or strategic inquiries via telephone, email, or web-portal. The Customer should retain a record of any Support Ticket number which may be provided by the Support Engineer.
3.4 The response and escalation times are dependent on the severity level of the Support Ticket as set out in the table below. Upon logging a Support Ticket with the Supplier's Support Engineer, an initial assessment shall be undertaken by the Supplier and a severity level discussed and agreed. The Customer should retain a record of any Support Ticket number which may be provided by the Support Engineer.
3.4.1 The Customer accepts that the vCISO/Consultancy service does not adhere to the SLA table for response times. The Supplier and Customer must agree on communication frequency during the service contract length and the frequency of scheduled meetings may increase or decrease depending on the outcomes that are outlined in the agreed-upon quote. The Supplier agrees to make best effort for availability for the duration of the contract.

TECH DRIVEN.
PEOPLE POWERED.

SERVICE LEVEL	DESCRIPTION	HOURS OF COVER	RESPONSE TIME	SEP2 INTERNAL ESCALATION ROUTE
1	**Platform / Service Impact** System Down. Production service or other mission-critical system(s) are down and no workaround is immediately available. This will impact all users	7 days a week 24 hours a day 24 x 7	SEP2 SOC team consolidate and verify event information and provide initial analysis within 15 minutes of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 Specialist team if further technical input or analysis is required or if the original issue is outstanding after 30 minutes. SEP2 Specialist team escalates to Vendor Support in cases of Platform issues.
2	**Platform / Service Impact** System is operating a degraded service to all users. One of more subsystems are not functioning or are impacting only a subset of users.	7 days a week 24 hours a day 24 x 7	SEP2 SOC team consolidate and verify event information and provide initial analysis within 1 hour of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 SIS/SAS team if further technical input or analysis is required or if the original issue is outstanding after 60 minutes. SEP2 Specialist team escalates to Vendor Support in cases of Platform issues.
3	**Platform / Service Impact** All major functionality is working. Non-critical	7 days a week 24 hours a day 24 x 7	SEP2 SOC team consolidate and verify event information and	SEP2 SOC escalate to SEP2 SIS/SAS team if further technical input or analysis

	system issues. Impaired operations of some components but allows the user to continue using the system.		provide initial analysis within 4 hours of initial report and begin further investigations or remedial actions as soon as technically able.	is required or if the original issue is outstanding after 8 hours. SEP2 Specialist team escalates to Vendor Support in cases of Platform issues.
4	**Platform / Service Impact** General enquiries. No service degradation.	7 days a week 24 hours a day 24 x 7	SEP2 SOC consolidate and verify event information and provide initial analysis within 8 hours of initial report and begin further investigations or remedial actions as soon as technically able.	SEP2 SOC escalate to SEP2 SIS/SAS team if further technical input or analysis is required or if the original issue is outstanding after 24 hours.

4. SERVICE DEPLOYMENT

4. SERVICE DEPLOYMENT
4.1 **Scoping and Strategy Session** - A planning session will be held between the Supplier and the Customer where specific requirements are captured and a working implementation plan is developed and agreed upon, as well as mutual agreement by both the Supplier and Customer as to timelines, milestones, and key dates to achieve transition to “live”. This will include the selection of compliance frameworks (e.g. NIST, ISO27001) and the definition of the "Strategy" roadmap. Neither party shall be unreasonable in providing agreement and sufficient resources to ensure that the timelines agreed are achievable.
4.2 **Tooling Configuration** - The Supplier shall configure the relevant GRC and Vulnerability Management modules (e.g. VMDR, CSAM, ETM) as defined in the Quotation.
4.2.1 Deployment of agents or virtual scanners is dependent on the Customer providing sufficient access to their infrastructure.
4.3 **Baseline Assessment** - The Supplier will conduct an initial discovery to classify known and unknown network assets perform a baseline Security Gap Analysis to establish the Customer's current posture score.
4.4 **Project Management** - Deployment milestones, such as "Audit Readiness" target dates, will be tracked using the Supplier’s project management tool (e.g. Halo), and will accessible to the Customer
4.5 The Supplier makes use of a project management tool, Halo, which it will allow the Customer access to, to be able to track and manage the process of the implementation. Exports from Halo can be taken via CSV/Excel as needed should the Customer need to manage data in their own environment.
4.5.1 The Supplier may use alternative specific tools from time to time at their discretion, so long as suitability of tools is largely inline with the functions that Halo provide.
4.5.2 After the planning and scoping session, the specific agreed tasks and milestones, capturing resourcing requirements from both the Supplier and the Customer will be added into the Halo project.
4.6 The Customer will ensure that they make available to the Supplier suitably experienced and authorised personnel to be able to facilitate the service implementation,
4.7 During the service implementation phase, and subject to mutual agreement to change the frequency, a weekly update meeting will be held. The scope of that meeting is from a project management perspective, to ensure that the

deployment is being completed as per the agreed plan created within the planning and scoping session.
4.7.1 Should any issues, dependencies, problems or other such be identified within this meeting, the respective party (either the Customer or the Supplier) will endeavor to provide further details and plans on how that can be remediated.
4.7.2 At a point which is mutually agreed upon by both the Supplier and the Customer, this scheduled update meeting can be stopped, at which point the service is deemed to have been deployed to live stage, and the service has entered into the business as usual phase.

4.8 During the implementation phase and thereafter as needed, the Supplier and the Customer will make use of the best possible methods of shared and communal communication, such as a shared Teams, Slack or Google Chat channel.

5. REPORTING & BUSINESS CONTINUITY

5.1 **Strategic Reporting** - The Supplier shall provide regular reporting as agreed in the Strategy Scoping session. This may include:
5.1.1 **Gap Analysis Reports** - Detailed breakdown of compliance status against chosen frameworks.
5.1.2 **Executive Reports** - High-level risk summaries suitable for Board presentation by the Dedicated Strategy Manager.
5.1.3 Vulnerability Reports - Metrics on detection, patch status, and risk reduction.
5.2 **Service Reviews** - The Supplier and Customer shall hold Service review meetings for the GRC service to review the Organisational Cyber Security Risk Strategy and adjust alignment as business needs evolve.
5.3 The Supplier shall implement a disaster recovery plan which sets out the Supplier's approach to ensure business continuity for the Services. The Supplier shall regularly carry out testing of its procedures for this purpose

6. SERVICE HANDOVER / EXIT TRANSITION

6.1 Irrespective of the methodology or reasons why a Termination (Clause 9 of the Terms and Conditions) has occurred, or in the case where the Contract is in its final month and is not intended to be extended/renewed by the Customer, the Supplier warrants that it shall act reasonably and with good faith to help and facilitate the Customer in the actions which may be required to support the Customer in moving to an alternative provider or platform.

6.2 **Tooling and Data**:
6.2.1 Any content created within the GRC platforms (policies, evidence links, asset classifications) specific to the Customer will be available for export, subject to the functionality of the third-party vendors (e.g. Drata, Qualys).
6.2.2 The Supplier will assist in the offboarding of the vCISO/Strategy Manager, including the revocation of access to Customer systems and the transfer of knowledge regarding the current Compliance Roadmap.
6.3 Asset Data: The Supplier will provide a final export of the Asset Inventory and Vulnerability data discovered during the contract term

7. THIRD PARTY SOFTWARE

7.1 Where the Wingman GRC quotation includes Drata, the Drata Terms and Conditions available at https://drata.com/terms fall within the scope of the EULA.
7.2 Where the Wingman GRC quotation includes Qualys or Vulnerability Management, the Qualys Terms and Conditions available at https://cdn2.qualys.com/docs/mktg/qualys-master-cloud-services-agreement.pdf fall within the scope of the EULA.

TECH DRIVEN.
PEOPLE POWERED.

Document Control Information

Document Details	
Document Title	SEP2 Terms and Conditions
Document Classification	Public
Date Last Saved	30/1/2026
Author	SEP2 Legal

Revision History

Revision #	Change description	Issue date
1.0	Fresh release of terms for 2026	30/1/26