



**4net Technologies Limited
and**

Master Agreement

27/07/2021

Contents

1.	Agreed Terms.....	3
2.	Agreement.....	9
3.	Conflict	10
4.	Commencement and Term	10
5.	Orders	10
6.	Price and Payments	10
7.	Amendment	13
8.	Invoice Payments	14
9.	Invoice Disputes	15
10.	Confidentiality.....	16
11.	Data Processing	17
12.	Intellectual Property Rights	18
13.	Limitation of Liability.....	19
14.	Termination.....	20
15.	Consequences of Termination.....	20
16.	Force Majeure	20
17.	Disputes Resolution Procedure	20
18.	General.....	21
19.	Supply Schedule	22
20.	Services Schedule	32
21.	The Order Schedule	45
22.	Annex to Standard Contractual Clauses.....	50

This Agreement is dated

PARTIES

- (1) **4NET TECHNOLOGIES LIMITED** incorporated and registered in England and Wales with company number 05448638 whose registered office is at 3 Scholar Green Road, Stretford, Manchester, Lancashire M32 0TR (**FourNet**); and
- (2) (Customer).

BACKGROUND

- (A) FourNet is a provider of various telecommunications and related services.
- (B) The Customer wishes to be provided with certain telecommunication services on the terms of this Agreement.

AGREED TERMS

INTERPRETATION

The following definitions apply in this Agreement:

Acceptance Tests: means those objective tests conducted by the Customer, which, when passed confirm that the Service or Installed Solution is accepted by the Customer and ready for use save for any minor non-conformities, which will be resolved as an Incident.

Additional Charges: all charges payable by the Customer in addition to Charges detailed in the Order with the Managed Services Schedule in addition to the annual Recurring Charge.

Administrator: means a person authorised by the Customer to manage MACDs and the passwords of Users and Agents.

Agent: means a Customer individual who is Provisioned to use the Contact Centre Applications and enabled to receive or make Calls using the Cloud Service.

Annual Charge: the annual charge for the Services as set out in the Order.

Applicable Law: means the laws of England and Wales and any laws and regulations, as may be amended from time to time, that apply to the provision or receipt of the Services and/or the Parties, including: applicable regulations of a Regulatory Body; anti-corruption laws set out in the Bribery Act 2010 and the Foreign Corrupt Practices Act of 1977 of the United States of America; and all applicable export laws and regulations, including those of the United States of America.

Applications: means Contact Centre (CC) Applications, Work Force Optimisation (WFO), Avaya Aura Experience Portal Application (AAEP), Interactive Voice Response services and applications (IVR) or Unified Communications (UC) Applications.

Availability: means the period of time when the Service is not Out of Service.

Avaya: means FourNet's supplier being a global supplier of business communications.

Billing Period: means a calendar month.

Business Day: a day other than a Saturday, Sunday, or public holiday in England when banks in London are open for business.

Call: means a signal, message or communication which can be silent, visual or spoken, excluding text messages.

Circuit: means any line, conductor, or other conduit between two terminals by which information is transmitted, and that is provided as part of the Service.

Claim: means any legal claims, actions, or proceedings against a Party, whether threatened or actual.

CLI: means the telephone number of the calling party or the default number of the Customer.

CLI Code of Practice: means the code by the same name as set out at <https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-industry-guidance/calling-line-identification>

Cloud Services: Services hosted in a FourNet data centre or a 3rd party supplier's data centre and provided to the Customer and managed by FourNet as set out in the Order.

Communications Provider or CP: means a 'Communications Provider' as defined in paragraph 1.4(a) of Condition 1 of the General Conditions of Entitlement set by Ofcom pursuant to section 45 of the Communications Act 2003.

Contact Centre or CC: means the suite of Software for providing contact centre services as set out in the Order.

Content: means applications, data, information (including emails), video, graphics, sound, music, photographs, software or any other material.

CPE: the customer premises equipment (such as routers, Network Terminating Equipment) which is provided by FourNet, or one of FourNet's suppliers (as the case may be), as set out in the Order.

CPS: means Carrier Pre-Selection.

CRF: is a Customer Requirement Form used by the Customer to either order the Cloud Service, or to modify certain aspects of the Cloud Service.

Customer Contact: has the meaning given in paragraph 5.3.1 of the Supply Schedule.

Customer Default: has the meaning any failure or delay by the Customer to perform any of the Customer's obligations under the agreement or the Order.

Customer Equipment: means any equipment (including software) other than FourNet Equipment, used by the Customer in connection with the Services.

Customer Service Plan or CSP: means the document of that name which sets out the procedures agreed between the Parties for managing disputes under this Agreement including any escalation process.

Delivery Location: the delivery location set out in the Order.

Domain Name: means a readable name on an Internet page that is linked to a numeric IP Address.

Due Date: has the meaning set out in clause 7.6.

E.164: means the ITU-T numbering plan for the world-wide public switched telephone network (PSTN).

Electronic Communications Network: has the meaning set out in the General Conditions of Entitlement found on the OFCOM Website.

Electronic Communications Service: has the meaning set out in the General Conditions of Entitlement found on the OFCOM Website.

Emergency: means a serious situation or occurrence that:

- (a) threatens life and limb; or
- (b) may cause or threatens to cause damage to physical property or systems; or
- (c) happens unexpectedly; and
- (d) demands immediate action.

Emergency Call: means a Call to 999 or 112.

Emergency Calls Access: means that component of the Services conveying Emergency Calls.

Emergency Services Database or ESDB: means the Emergency Call routing and address database.

Emergency Services Organisation: means the relevant local public police, fire, ambulance and coastguard services and other similar organisation.

Enabling Service: has the meaning given in 5.2.5 of the Services Schedule.

Equipment: the equipment to which the Services apply as set out in the Order.

First Response: FourNet have received and logged the Incident and passed to a Resolver Group.

FourNet Equipment: means any equipment, including any Software, owned or licensed by FourNet or its sub-contractors, that is located at a Site for the provision of the Service(s) and, if any, as more fully described in the Supply Schedule and set out in an Order.

Goods: the goods (or any part of them) set out in the Order.

.

Implementation Services: means the supply, installation, configuration and programming of the Equipment and or the Services and training where set out in the Order.

Incident: an unplanned interruption to a Service or reduction in the quality of a Service.

Incoming Call: means a Call from destinations with E.164 numbers made to a User.

Intellectual Property Rights: means all patents, rights to inventions, utility models, copyright and related rights, trademarks, service marks, trade, business and domain names, rights in trade dress or get-up, rights in goodwill or to sue for passing off, unfair competition rights, rights in designs, rights in computer software, database rights, topography rights, rights in confidential information (including know-how and trade secrets) and any other intellectual property rights, in each case whether registered or unregistered and including all applications for, and renewals or extensions of, such rights, and all similar or equivalent rights or forms of protection in any part of the world.

Initial Term: means the length of the contract term for the Service procured as set out in the Order.

Internal Calls or On-Net: means Calls made between Users configured within the Customer where both Users are using IP phones (hard or soft).

International Destination Network: means a network operated in an overseas country.

Internet: means a global system of interconnected networks that use a standard Internet Protocol to link devices worldwide.

Internet Protocol or IP: means a communications protocol for devices connected to the Internet that specifies the format for addresses and units of transmitted data.

IP Address: means a unique number on the Internet of a network card or controller that identifies a device and is visible by all other devices on the Internet.

IP Network: means a telecommunications network operated on IP.

IVR Port: means an Interactive Voice Response port on the Avaya Experience Portal.

Local Area Network or LAN: means the infrastructure that enables the ability to transfer IP services within Sites (including data, voice, and video conferencing services).

MACD: means moves, adds, changes, and deletes carried out on the Applications by the Administrator.

Managed Services: the managed services to be provided by FourNet as set out in the Order.

Manufacturer Support Charges: the charges for the maintenance services or software assurance provided by the manufacturer of the Goods as set out in the Order.

Manufacturer Software: software developed, supported and tested by a 3rd party supplier.

Measurement Period: means a calendar month (24 hours per day).

Minimum Billable Value: means the lowest charges reflected within the commercial offer of the Order based upon the Minimum Billable Volume of Monthly Usage.

Minimum Billable Volume: refers to the lowest volume of licenses reflected within the commercial offer of the Order. Where Monthly Usage drops below the agreed volume, the Minimum Billable Value shall be charged.

Monthly Usage: means in relation to:

- (a) Contact Centre Applications – the concurrent peak number of Users logged in to the applicable Contact Centre Applications, measured across the Customer's entire base of Users, over the Measurement Period.
- (b) WFO and WFM Applications – this the highest number of named Agents, for whom the applicable WFO Application is Provisioned, that are configured into the Contact Centre (as measured by the Service Portal), during the Measurement Period; and
- (c) UC Applications – the concurrent peak number of Users Provisioned on the applicable UC Application, measured across the Customer's entire base of Users, over the Measurement Period (measured by the Service Portal).

Network Services: means the provision of the existing telephone lines and telephony services and the new telephone lines and telephony services, wide area network (WAN) services, the SIP Services, CPS and other ancillary services which are all as set out in the Order.

Number Portability: means an arrangement whereby a Customer's telephone number ceases to be provided by the losing CP and such Customer telephone number is subject to number import onto the Cloud Service. If the Customer telephone number ceases to be used by FourNet then it may be subject to number export to the gaining CP pursuant to the Number Portability rules as set out in the Product Handbook.

Ofcom: means the Office of Communications or its successor body or authority that is the regulatory body for communications in the UK.

On-Net or Internal Calls: means Calls made between Users configured within the Customer where both Users are using IP phones (hard or soft).

Operating Services Manual: means a detailed document that is produced in collaboration with the Customer during Service Transition, that covers all aspects of the delivery of the Managed Services.

Order: means the Customer's order for the Goods and/or Services as set out in Order Schedule to this Agreement and any further orders as agreed between the parties which refer to this Agreement and which shall be in a substantially similar form to the order set out in the Order Schedule.

Out of Service: means an outage affecting more than 20% (but not less than 20) of the Customer's Users for the applicable Application, excluding outages for Planned Maintenance or Emergency maintenance.

Planned Maintenance: means any work planned in advance to be carried out by, or on behalf of, FourNet, including:

- (a) to maintain, repair or improve the performance of FourNet's network (or that of FourNet's subcontractors) or any Services; or
- (b) to make any change to the Services that does not have a material adverse effect on the performance or provision of the Cloud Service including: the introduction or withdrawal of any Service features; or the replacement of any Service with an equivalent Service.

Presentation Number: means the telephone number made available to a called party.

Price or Charges: means the price for the Goods and/or Services as set out in the Order.

Professional Services: means one off implementation and training services delivered to the Customer by FourNet or a 3rd Party on behalf of FourNet, these services are further defined in the Services Schedule.

Provisioned: means enabled by the Customer using a Service Portal to log on and use the applicable Application.

Premium Rate Service: means a communications service where Call Charges include a premium to cover the cost of content and/or an element of the service above the costs and Charges attributable to conveyance.

PSTN: means Public Switched Telephone Network, which is the concentration of the world's public circuit switched telephone networks.

Recurring Charges: means Charges for the Services or applicable part of the Services that are invoiced repeatedly in every payment period (e.g. every month, every quarter, or annually), as set in the Order.

Recurring Invoice Date: means the date specified in the Order which will be the date the first invoice will be raised for a Recurring Charge. If no such date is specified in the Order, then the date shall be the date of last signature of the Order.

Regulatory Body: means any national or supranational regulatory or competition body, government department, court, or other body authorised and empowered under local law in the relevant country to regulate or adjudicate on the provision of the Services.

Renewal Period: means a period equivalent to the shorter of (i) the Initial Period and (ii) 3 years.

Resolver Group: means Tier 2 and 3 FourNet engineers, supporting 3rd parties or any other relevant person to investigate and solve a customer query or incident.

Scope of Work: means the document described as such to be provided by FourNet detailing the Services to be carried out by FourNet

Second Response: Resolver Group are actively engaged in fault investigation, logged on to relevant systems and engaged with the Customer.

Services: means the Managed Services, Cloud Services and Network Services as appropriate.

Service Delivery Date: means the date that the Service is available to the Customer and the charges for the, Cloud and Manufacturer Support will be charged from. This is the later date of 90 days following order placement or the Service being available for User Acceptance Testing (unless otherwise specified in the Order).

Service Credit: means any agreed remedy for failure by FourNet to meet a Service Level for the Service set out in an Order.

Service Level: means any agreed minimum level of Service to be achieved by FourNet with respect to the Service, such as delivery, availability or restoration as set out in the Services Schedule. Bespoke Service Levels will be described in the Order.

Service Management Boundary: has the meaning given in paragraph 7 of the Services Schedule.

Service Portal: means the portal used by the Supplier to administer the Services and configure Applications and to create and receive reports on the utilisation of the Services.

Service Transition: means the process adopted when a project nears completion and the ongoing support services begin. This also covers the process when a Customer orders services that are not attached to a project, where the procured Goods or Services require ongoing maintenance and support.

SIP Services: means a Voice over Internet Protocol (VoIP) service based on the Session Initiation Protocol (SIP) by which FourNet delivers telephone connectivity to the public switched telephone network (PSTN) to the Customer with a compatible phone system (IP-PBX) as set out in the Order.

Sites: means the locations set out in the Order.

Software: means any software installed on or supplied with the Goods or as set out on the Order.

Specification: means any specification for the Goods issued by the manufacturer.

Statement of Work: means the detailed plan describing the Services required to fulfil the Order. (if any).

Supervisor: means an individual whose role at the Customer's organisation includes the management of Agents and requires access to the supervisor management and reporting tools.

Support Hours: the hours of support set out in the Order.

Target Restoration: the FourNet target to have Service(s) restored to a usable working state by means of full fault fix or the implementation of a workaround.

UC Applications: means the Software for the provision of unified communications services as set out in the Order.

Uniform Resource Locator or URL: means a character string that points to a resource on an intranet or the Internet.

Usage Charges: means the Charges for the Outgoing Calls services as specified in the Order.

User: means any person who is permitted by the Customer to use or access the Services.

VAT: Value Added Tax chargeable under English law for the time being and any similar additional tax.

Voice Channel: means the capacity needed to carry a single Call.

VOIP: means voice over internet protocol.

WFO Applications: means applications supporting work force optimisation including call recording, quality monitoring and workforce management.

Working Day: means 8.30 to 17.30 Monday to Friday, excluding public or bank holidays in the applicable part of the United Kingdom.

3rd Party Supplier: a supplier or sub contractor used by FourNet to deliver part or all of the Professional Services or other Services detailed in the Order.

Clause, schedule, and paragraph headings shall not affect the interpretation of this Agreement.

A person includes a natural person, corporate or unincorporated body (whether or not having separate legal personality) and that person's legal and personal representatives, successors and permitted assigns.

1. AGREEMENT

- 1.1 The schedules form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the schedules.
- 1.2 A reference to a company shall include any company, corporation, or other body corporate, wherever and however incorporated or established.

- 1.3 Unless the context otherwise requires, words in the singular shall include the plural and, in the plural, shall include the singular.
- 1.4 Unless the context otherwise requires, a reference to one gender shall include a reference to the other genders.
- 1.5 A reference to a statute or statutory provision is a reference to it as amended, extended, or re-enacted from time to time.
- 1.6 A reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.
- 1.7 References to Clauses and Schedules are to the clauses and schedules of this Agreement; references to Appendices and paragraphs are to appendices and paragraphs of the relevant Schedule.
- 1.8 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, description, definition, phrase or term preceding those terms.

2. CONFLICT

- 2.1 The provisions of the main body of this Agreement shall be supplemented by any applicable additional provisions set out in the Schedules.
- 2.2 In the event, that any provision of the main body of this Agreement conflicts with any provision of any Schedule, the provisions of the Schedule shall take precedence.

3. COMMENCEMENT AND TERM

- 3.1 This Master Agreement commences on the date hereof and, subject to paragraph 13, shall continue until terminated by either party in accordance with paragraph 13 or clause 3.5.
- 3.2 FourNet will provide each Service from its Service Delivery Date for the duration of the Initial Term and thereafter for each Renewal Period.
- 3.3 Either party may give written notice to the other party not less than 90 days before the end of the Initial Term or the relevant Renewal Period of the Order to terminate the Service at the end of the Initial Term or the relevant Renewal Period as the case may be.
- 3.4 Either party may give written notice to the other party with no less than 90 days before the intended termination date of the Master Agreement. Orders signed under this Agreement shall complete the Initial Term or relevant Renewal Period before the termination comes into effect.

4. ORDERS

- 4.1 When the Customer wishes FourNet to provide it with Goods and/or Services, it shall send an Order to FourNet. Each Order shall be deemed to be a separate offer by the Customer to purchase Services on the terms of this Agreement, which FourNet shall be free to accept or decline at its absolute discretion.
- 4.2 No Order shall be deemed to be accepted by FourNet until it issues a written acceptance of the Order or (if earlier) FourNet commences provision of the Services to the Customer.
- 4.3 Each Order shall refer to this Agreement and be deemed to incorporate all provisions of this Agreement, save as expressly varied in the Order.

5. PRICE AND PAYMENT

- 5.1 Unless otherwise stated in the Order, Charges are due from the Customer to the Supplier in accordance with clauses 5.1.1 and 5.1.2 below:
- 5.1.1 all Recurring Charges shall be invoiced on the Recurring Invoice Date. Where such Recurring Charges are payable monthly then the subsequent invoices will be sent on the same date of each subsequent month as the Recurring Invoice Date; where the Recurring Charges are annual the subsequent invoices shall be sent on each anniversary of the Recurring Invoice Date; where the Recurring Charges are quarterly the subsequent invoices shall be sent on the last day of the quarter of the Recurring Invoice Date, and on the last day of each quarter thereafter. ;
- 5.1.2 all other Services, Professional Services and services including but not limited to the provision of any Perpetual Software licences or Equipment, shall be invoiced in accordance with the dates and/or Milestones (as applicable) set out in the Order.
- 5.2 The full balance of the Order value of any Goods is due on the earlier of (i) the date of delivery of the Goods to the Customer premises or the Delivery Location, if different, (ii) the date that FourNet notifies the Customer that the Goods are available for delivery to the Customer's premises or (iii) the date of delivery to FourNet in circumstances where FourNet is to carry out configuration or other services to such Goods at FourNet premises.

Managed Service and Cloud Service Charges

- 5.3 The Price for the Services shall be inclusive of the Manufacturer Support Charges, the Annual Charge and any Cloud, Rental, Subscription or Network Services Charges unless otherwise stated.
- 5.4 Not Used..
- 5.5 Not Used.
- 5.6 Not Used. .

Professional Services Charges

- 5.7 Where Professional Services are provided on a fixed price basis:
- 5.7.1 Cancellation or rescheduling of the services set out in the Scope of Work by the Customer will incur Additional Charges;
- 5.7.2 Where the Professional Services are provided on a time-and-materials basis:
- 5.7.3 FourNet's standard daily rates are calculated on the basis of a day worked between 9.00 am and 5.30 pm on weekdays (excluding weekends and public holidays);
- 5.7.4 FourNet shall be entitled to charge at an overtime rate of 150% of the normal rate for time worked by members of the project team outside the hours referred to in paragraph 5.7 and on Saturdays and 200% of the normal rate on Sundays and public holidays;
- 5.8 FourNet shall invoice the Customer as set out in the Order for its charges for time, expenses, and materials (together with VAT where appropriate) for the month concerned, calculated as provided in this paragraph 5.8. Each invoice shall set out the time spent by each member of the project team and provide a detailed breakdown of any expenses and materials, accompanied by the relevant receipts.
- 5.9 All payments payable to FourNet for any services provided hereunder shall become due immediately on termination of this Agreement, despite any other provision.

6. Amendment

- 6.1 Save as set out in clauses 6.2, no amendment of the Order will be effective unless agreed in writing by the Parties.
- 6.2 FourNet may amend the Order at any time by giving the Customer 21 days' notice in order to:
- 6.2.1 comply with any legal or regulatory obligation; or
 - 6.2.2 protect the use of its brand or that of its subcontractors; or
 - 6.2.3 introduce new or improved service features; or
 - 6.2.4 withdraw service features or components; or
 - 6.2.5 introduce new or improved service levels; or
 - 6.2.6 change the technical specification of the Services; or
 - 6.2.7 improve clarity, or make corrections to typographical errors; or
 - 6.2.8 introduce process changes; or
 - 6.2.9 change the codes or the numbers allocated to the Services in order to meet the national numbering requirements of Ofcom;
- 6.3 FourNet will provide 21 days' notice if it proposes any amendments to the Order that are not otherwise specifically referred to in this Agreement.
- 6.4 Upon expiry of the notice the changes to the Order proposed by FourNet will automatically apply unless the Customer responds to FourNet within 28 days of the notice disagreeing with the changes.

7. Invoice Payment

- 7.1 The Customer shall pay each invoice submitted by FourNet:
- 7.1.1 within 30 days of the date of receipt of the invoice; and
 - 7.1.2 in full and in cleared funds to a bank account in the name of 4net Technologies Limited.
- 7.2 Any Charges (which shall be pre-approved by customer) include the cost of hotel, subsistence, travelling, and any other ancillary expenses reasonably incurred by FourNet in connection with the Services, and the cost of any materials or services reasonably and properly provided by third parties required by FourNet for the supply of the Services unless otherwise stated on the Order.
- 7.3 The Charges are exclusive of VAT (if applicable), which FourNet shall add to its invoices at the appropriate rate.
- 7.4 Where invoices are to be issued online, FourNet will notify the Customer by email when a new invoice is issued.
- 7.5 Without limiting any other right or remedy of FourNet, if the Customer fails to make any payment due to FourNet under this Agreement by the due date for payment (Due Date):
- 7.5.1 FourNet shall have the right to charge interest on the overdue amount at the rate of 3 per cent per annum above the then current Barclays Bank plc's base lending rate accruing on a daily basis from the Due Date until the date of actual payment of the overdue amount, whether before or after judgment, and compounding annually; and
 - 7.5.2 FourNet may suspend the Services or Professional Services until payment has been made in full.
- 7.6 The Customer shall pay all amounts due under this Agreement in full without any deduction or withholding except as required by law and the Customer shall not be entitled to assert any credit, set-off or counterclaim against FourNet in order to justify withholding payment of any such amount in whole or in part. FourNet may, without limiting its other rights or remedies, set off any amount owing to it by the Customer against any amount payable by FourNet to the Customer.

- 7.7 Where the Customer makes an aggregated payment in respect of more than one invoice, the Customer will, upon request, provide a breakdown to show amounts paid in relation to each individual invoice, clearly identifying the amount applicable to each.
- 7.8 In the event, that the price to FourNet of any Goods, Cloud Services, Network Services or Software Assurance increases by more than 2% due to a fall in the sterling exchange rate or due to an increase in the rate of inflation (as documented by the Office of National Statistics) from that of the date of the relevant Order, FourNet may on notice to the Customer increase the Price by the increase to FourNet of the same.
- 7.9 Where FourNet has issued an incorrect invoice, FourNet may issue an amending invoice or credit note together with details of the error to the Customer within 3 months of the issuing of the incorrect invoice.

8. Invoice Disputes

- 8.1 The Customer will pay by the Due Date, all undisputed amounts.
- 8.2 If the Customer disputes an invoice, it will provide Notice to FourNet of the dispute within 14 days of the date of the invoice and will provide all information relevant to the dispute, stating the reasons for and the amount in dispute.

If the Customer pays by direct debit, FourNet will amend the direct debit by the disputed amount while it investigates the dispute.

- 8.3 The Customer will pay any resolved amount within five Business Days after the resolution of the dispute.
- 8.4 Paragraph 8 will apply to any resolved amounts payable to FourNet from the original Due Date.

9. CONFIDENTIALITY

- 9.1 Each party shall keep in strict confidence all confidential information concerning the business, affairs, customers, clients or suppliers of FourNet disclosed to the other party, its agents or employees. The Customer 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 its obligations to the other Party and shall ensure that such employees, agents, or sub-contractors are subject to obligations of confidentiality corresponding to those which bind the Parties.

All materials, equipment and tools, drawings, specifications, and data supplied by FourNet to the Customer shall at all times be and remain the exclusive property of FourNet but shall be held by the Customer in safe custody at its own risk and maintained and kept in good condition by the Customer until returned to FourNet, and shall not be disposed of or used other than in accordance with FourNet's written instructions or authorisation.

- 9.2 This clause shall survive termination of this Agreement, howsoever arising.

10. DATA PROCESSING

- 10.1 In this Clause 10:

- 10.1.1 "Data Protection Law": means the General Data Protection Regulation 2018 ("GDPR") and the Data Protection Act 2018 and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner from time to time;
- 10.1.2 "process", "data controller", "data processor", "data subject(s)", "personal data", and "subject access request" shall have the meaning given in the Data Protection Law.

- 10.2 The Customer will comply with its obligations as a data controller under Data Protection Law. The Customer warrants and represents that the carrying out by FourNet of processing of the personal data under this Agreement shall not infringe Data Protection Laws.
- 10.3 The Customer hereby appoints FourNet as data processor in relation to personal data which FourNet receives under or in connection with the performance of this Agreement.
- 10.4 FourNet warrants and represents that it will comply with its obligations under the Data Protection Laws
- 10.5 The details of the personal data processed for the purposes of this Agreement include:
- 10.6 Subject matter: The subject matter of the data processing is the carrying out of the Services under this Agreement.
- 10.7 Duration: The duration of the data processing is until the termination of the Agreement in accordance with its terms.
- 10.8 Purpose: The purpose of the data processing is the provision of the Services to the Customer and the performance of FourNet's obligations under the Agreement or as otherwise agreed by the Parties.
- 10.9 Nature of the processing: Using personal data in the performance of the Services.
- 10.10 Categories of data subjects: Employees of the Customer.
- 10.11 Types of personal data: Contact details of the data subjects.
- 10.12 In processing personal data pursuant to this Agreement, FourNet shall:
- 10.12.1 act only on documented instructions from the Customer unless required to do so by Data Protection Law, in which case FourNet shall inform the Customer of such legal requirement before carrying out such processing, unless that law prohibits the provision of such information on grounds of public interest;
 - 10.12.2 ensure that all FourNet personnel involved in the processing of personal data (including its staff, agents and subcontractors) are under appropriate obligation of confidentiality;
 - 10.12.3 take all measures required by Article 32 of the GDPR in respect of the personal data;
 - 10.12.4 not engage another processor without the prior written authorisation of the Customer. Where FourNet does engage another processor, FourNet shall impose the same obligations on such processor as are imposed on FourNet by this clause 10.11.4;
 - 10.12.5 taking 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 subject's rights set out in Chapter III of the GDPR;
 - 10.12.6 assist the Customer in ensuring compliance with the obligations set out in Articles 32 to 36 of the GDPR taking into account the nature of the processing and the information available to FourNet;
 - 10.12.7 at the Customer's choice, delete or return to Customer all personal data in its possession or control after the end of such processing, save that this requirement shall not apply to the extent FourNet is required by Data Protection Law to retain some or all of the personal data.
 - 10.12.8 make available to the Customer all information necessary to demonstrate compliance with this Agreement and allow the Customer (or its authorised representatives) to inspect and audit FourNet's compliance with the terms of this Agreement;
 - 10.12.9 notify the Customer immediately if, in FourNet's opinion an instruction from the Customer infringes Data Protection Law

- 10.12.10 not cause or permit personal data to be transferred outside the EU without the Customer's prior written consent, unless required to do so by Data Protection Law.
- 10.12.11 Ensure that if FourNet transfers personal data to sub-contractors located in countries outside the EEA, that transfer shall be subject to the terms of the Standard Contractual Clauses (as per European Commission's Decision 2010/87/EU) as set out in Annex 2 which FourNet enters into on behalf of the sub-contractor with the Customer.

11. INTELLECTUAL PROPERTY RIGHTS

- 11.1 The Customer acknowledges that all Intellectual Property Rights subsisting in the Goods are and shall remain the sole property of FourNet or (as the case may be) third party rights owner. This does not apply to Intellectual Property Rights belonging to the Customer.
- 11.2 In relation to the Software:
- 11.3 the Customer acknowledges that it is buying only the media on which the software is recorded and the accompanying user manuals;
- 11.4 nothing contained in this Agreement shall be construed as an assignment of any Intellectual Property Rights in the Software or user manuals; and
- 11.5 the Customer shall be subject to the rights and restrictions imposed by the owner of the Intellectual Property Rights in the Software and user manuals, and shall comply with all licences, terms of use and registration requirements relating to them. The end user licence terms for 3rd Party Software are included in the Annex to the relevant Schedule.
- 11.6 Each Party's Intellectual Property Rights, whether pre-existing or created by a Party during or arising out of or in connection with the performance of this Order, will remain the absolute property of that Party or its licensors.
- 11.7 In reference to Cloud Services, FourNet will give the Customer a non-transferable and non-exclusive licence to use, solely as necessary for receipt or use of the Cloud Service(s), all Software (in object code form only) and associated documentation that may be supplied by FourNet, subject to the Customer's compliance with this Agreement and any third party terms and conditions, as more fully set out in this Agreement or set out in an Order, that apply to the use of the Software. Such licenses will terminate at the end of the term.
- 11.8 The Customer will not copy, decompile, modify, or reverse engineer any Software or knowingly allow or permit anyone else to do so, except as expressly permitted by FourNet in writing or otherwise provided at law.
- 11.9 FourNet will indemnify, hold harmless and defend the Customer from and against any Claims brought against it by a third party for alleged infringement of that third party's Intellectual Property Rights by the Customer's receipt of any Service(s) provided that, for each Claim, the Customer promptly notifies FourNet of the Claim, FourNet is given immediate and complete control of the Claim, the Customer does not make any public statements related to the Claim or in any way prejudice FourNet's defence of the Claim, and the Customer gives FourNet (or its subcontractors) all reasonable assistance with the Claim. All costs incurred or recovered in negotiations, litigation, and settlements relating to any indemnity given under this clause 11.9 will be for FourNet's account.
- 11.10 The indemnity set out in paragraph 11.9 will not apply to Claims arising out of or in connection with:
 - 11.10.1 the use of any Service in conjunction or combination with other equipment or software or any other service(s) not supplied by FourNet;
 - 11.10.2 any unauthorised alteration or modification of any Service;
 - 11.10.3 content, designs, or specifications supplied by, or on behalf of, the Customer; or
 - 11.10.4 use of the Services other than in accordance with this Agreement.

- 11.11 The Customer will indemnify FourNet against all Claims, losses, costs and liabilities arising out of or in connection with the matters set out in clause 11.10 that are attributable to the Customer or its agents or Users and will cease any such activity immediately upon notice from FourNet or at such time as the Customer became aware, or should have reasonably have been aware, that the activity had given rise to the Claim.
- 11.12 If any Service becomes, or FourNet reasonably believes it is likely to become, the subject of a Claim of infringement of any third party's Intellectual Property Rights as referred to in clause 11.9, FourNet may, at its own expense:
- 11.12.1 secure for the Customer a right of continued use; or
 - 11.12.2 modify or replace the relevant part(s) of the Services so that it is no longer infringing, provided that that modification or replacement will not materially affect the performance of the relevant part(s) of the Services.
- 11.13 The indemnity in clause 11.9 and the actions in clause 11.12 will be the Customer's sole and exclusive remedy for any Claims arising out of or in connection with an infringement of Intellectual Property Rights.
- 11.14 FourNet represents and warrants that:
- 11.14.1 the Services will be performed with reasonable care and skill and in accordance with good industry practice;
 - 11.14.2 it will endeavour to act in good faith in delivering the Services to the Customer;
 - 11.14.3 in performing its obligations under this Agreement it will maintain all necessary regulatory and governmental: licenses, consents, and permissions;
 - 11.14.4 it will maintain in force, with a reputable insurance company, all necessary insurances to cover the liabilities that may arise under or in connection with this Agreement;
 - 11.14.5 it will comply with all applicable laws and regulations with respect to its obligations under this Agreement; and
 - 11.14.6 it will notify the Customer in writing as soon as reasonably practicable upon the occurrence of a change of control.

12. LIMITATION OF LIABILITY

- 12.1 The following provisions set out the entire financial liability of the Parties (including without limitation any liability for the acts or omissions of its employees, agents, and sub-contractors) in respect of:
- 12.1.1 any breach of this Agreement howsoever arising;
 - 12.1.2 any representation, misrepresentation (whether innocent or negligent), statement or tortious act or omission (including without limitation negligence) arising under or in connection with this Agreement.
- 12.2 Nothing in this Agreement shall limit or exclude a Party's liability for:
- 12.2.1 death or personal injury caused by its negligence, or the negligence of its employees, agents or subcontractors; the indemnity provided in clause 11.9;
 - 12.2.2 a Party's payment obligations;
 - 12.2.3 a breach of a party's confidentiality obligations;
 - 12.2.4 fraud or wilful negligence;
 - 12.2.5 fraud or fraudulent misrepresentation; or

- 12.2.6 breach of the terms implied by section 2 of the Supply of Goods and Services Act 1982 (title and quiet possession); or
 - 12.2.7 any matter in respect of which it would be unlawful for FourNet to exclude or restrict liability.
- 12.3 Subject to clause 12.1 and clause 12.2:
- 12.3.1 A Party shall not be liable to the other Party, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, for any of the reasons listed below arising under or in connection with this Agreement:
 - 12.3.1.1 loss of profit; or
 - 12.3.1.2 loss of business; or
 - 12.3.1.3 depletion of goodwill or similar losses; or
 - 12.3.1.4 loss of anticipated savings; or
 - 12.3.1.5 loss of contract; or
 - 12.3.1.6 loss of use; or
 - 12.3.1.7 loss or corruption of data or information; or
 - 12.3.1.8 any special, indirect, or consequential loss; and
 - 12.3.1.9 A Party's aggregate liability to the other Party arising under or in connection with this Agreement in each consecutive 12 month period commencing on the date hereof, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, shall not exceed the total Price paid or payable by the Customer during that period.
- 12.4 The Customer shall be responsible for putting in place and maintaining all necessary technical and other measures to ensure the security of its networks and systems (including the Equipment). The Customer acknowledges and agrees that FourNet shall have no liability in respect of any unauthorised use of the Customer's networks and systems (including the Equipment) The Customer shall be responsible for all sums due to third parties for the use of third parties such as communications providers for use of their systems.
- 12.5 Except as set out in this Agreement, all warranties, conditions, and other terms implied by statute or common law are, to the fullest extent permitted by law, excluded from this Agreement.
- 12.6 The parties agree that, in entering into this Agreement, either it did not rely on any representations (whether written or oral) of any kind or of any person other than those expressly set out in this Agreement or (if it did rely on any representations, whether written or oral, not expressly set out in this Agreement) that it shall have no remedy in respect of such representations and (in either case) the other party shall have no liability in any circumstances otherwise than in accordance with the express terms of this Agreement.
- 12.7 Any amounts paid by FourNet to the Customer as Service Credits, as may be more fully described in the applicable Order, will be the Customer's sole and exclusive remedy for any failure by FourNet to meet an applicable Service Level and, in any case, will reduce any damages payable up to the applicable limits of liability.
- 12.8 This clause 12 shall survive termination of this Agreement.

13. TERMINATION

- 13.1 Without limiting its other rights or remedies, either party may terminate this Agreement with immediate effect by giving written notice to the other party if:

- 13.1.1 the other party commits a material breach of this Agreement and (if such a breach is remediable) fails to remedy that breach within 30 days of that party being notified in writing of the breach;
 - 13.1.2 the other party suspends, or threatens to suspend, payment of its debts or is unable to pay its debts as they fall due or admits inability to pay its debts or (being a company) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986 or (being an individual) is deemed either unable to pay its debts or as having no reasonable prospect of so doing, in either case, within the meaning of section 268 of the Insolvency Act 1986 or (being a partnership) has any partner to whom any of the foregoing apply;
 - 13.1.3 the other party commences negotiations with all or any class of its creditors with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with its creditors other than (where a company) for the sole purpose of a scheme for a solvent amalgamation of that other party with one or more other companies or the solvent reconstruction of that other party;
 - 13.1.4 a petition is filed, a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of that other party (being a company) other than for the sole purpose of a scheme for a solvent amalgamation of that other party with one or more other companies or the solvent reconstruction of that other party;
 - 13.1.5 a creditor or encumbrancer of the other party attaches or takes possession of, or a distress, execution, sequestration or other such process is levied or enforced on or sued against, the whole or any part of its assets and such attachment or process is not discharged within 14 days;
 - 13.1.6 an application is made to court, or an order is made, for the appointment of an administrator or if a notice of intention to appoint an administrator is given or if an administrator is appointed over the other party;
 - 13.1.7 a floating charge holder over the assets of that other party has become entitled to appoint or has appointed an administrative receiver;
 - 13.1.8 a person becomes entitled to appoint a receiver over the assets of the other party or a receiver is appointed over the assets of the other party;
 - 13.1.9 any event occurs or proceeding is taken with respect to the other party in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned in clause 13.1.2 to clause 13.1.8 (inclusive);
 - 13.1.10 the other party suspends or ceases, or threatens to suspend or cease, to carry on all or a substantial part of its business.
- 13.2 Without limiting its other rights or remedies, FourNet may terminate this Agreement with immediate effect by giving written notice to the Customer if the Customer fails to pay any amount due under this Agreement by the Due Date and remains in default not less than 28 days after being notified in writing to make such payment.
- 13.3 Without limiting its other rights or remedies, FourNet shall have the right to suspend provision of the Services under this Agreement or any other contract between the Customer and FourNet if the Customer becomes subject to any of the events listed in clause 13.1.1 to clause 13.1.10, or if the Customer fails to pay any amount due under this Agreement on the due date for payment.

14. CONSEQUENCES OF TERMINATION

- 14.1 On termination of this Agreement for any reason:
 - 14.1.1 the Customer shall within 7 days to FourNet all of FourNet's outstanding unpaid invoices and interest and, in respect of Services supplied but for which no invoice has

been submitted, FourNet shall submit an invoice, which shall be payable by the Customer within 7 days of receipt;

- 14.1.2 all rights and licences granted to the Customer pursuant to the Agreement shall cease;
- 14.1.3 the Customer shall return or allow FourNet to enter the Customer's premises to collect, all FourNet Equipment.
- 14.1.4 the accrued rights, remedies, obligations, and liabilities of the parties as at expiry or termination shall not be affected, including the right to claim damages in respect of any breach of this Agreement which existed at or before the date of termination or expiry; and
- 14.1.5 clauses which expressly or by implication have effect after termination shall continue in full force and effect.

15. FORCE MAJEURE

- 15.1 Neither party shall be liable for any failure or delay in performing its obligations under this Agreement to the extent that such failure or delay is caused by an event beyond a that party's reasonable control, which by its nature could not have been foreseen, or, if it could have been foreseen, was unavoidable. Should a force majeure event subsist for more than 30 days the Party not claiming force majeure may terminate this agreement on 7 days written notice.

16. DISPUTE RESOLUTION PROCEDURE

- 16.1 If a dispute arises out of or in connection with this Agreement or the performance, validity, or enforceability of it ("Dispute"), then, except as expressly provided in this Agreement, the parties shall follow the procedure set out in this clause:
 - 16.1.1 either party may give to the other written notice of the Dispute, setting out its nature and full particulars ("Dispute Notice"), together with relevant supporting documents. On service of the Dispute Notice, the [EMPLOYEE TITLE] of FourNet and [EMPLOYEE TITLE] of the Customer shall attempt in good faith to resolve the Dispute.
 - 16.1.2 if the parties are for any reason unable to resolve the Dispute through the process set out in clause 16.1.1 within 30 days of service of the Dispute Notice, the Dispute shall be referred to the [SENIOR OFFICER TITLE] of FourNet and [SENIOR OFFICER TITLE] of the Customer who shall attempt in good faith to resolve it; and
- 16.2 if the parties are for any reason unable to resolve the Dispute within 30 days of it being referred pursuant to clause 16.1, the parties agree to enter into mediation in good faith to settle the Dispute in accordance with the CEDR Model Mediation Procedure. Unless otherwise agreed between the parties within 60 days of service of the Dispute Notice, the mediator shall be nominated by CEDR. To initiate the mediation, a party must serve notice in writing (ADR notice) to the other party to the Dispute, referring the dispute to mediation. Unless otherwise agreed between the parties, the mediation will start not later than 14 days after the date of the ADR notice.
- 16.3 The commencement of mediation shall not prevent the parties commencing or continuing court proceedings in relation to the Dispute under clause 17.9 (Governing law and jurisdiction).
- 16.4 If the Dispute is not resolved within 14 days after service of the ADR notice, the Dispute shall be finally resolved by the courts of England and Wales in accordance with clause 17.9 (Governing law and jurisdiction).

17. GENERAL

- 17.1 **Entire agreement:** This Agreement constitutes the entire agreement between the parties. The Customer acknowledges that it has not relied on any statement, proposal, promise or representation made or given by or on behalf of FourNet which is not set out in this Agreement. Any proposal, samples, drawings, descriptive matter or advertising issued by FourNet, and any descriptions or illustrations contained in FourNet's catalogues or brochures, are issued or published for the sole purpose of giving an approximate idea of the Goods and/or Services described in them. They shall not form part of this Agreement or any other contract between FourNet and the Customer for the supply of the Goods and/or Services.
- 17.2 **Assignment and subcontracting:** Neither Party shall assign, transfer, charge, subcontract or deal in any other manner with all or any of its rights or obligations under this Agreement.
- 17.3 **Notices:** Any notice or other communication required to be given to a party under or in connection with this Agreement shall be in writing and shall be delivered to the other party personally or sent by prepaid first-class post, recorded delivery, by commercial courier, at its registered office (if a company) or (in any other case) its principal place of business, or by email at the email address notified by the receiving party in a notice to the other party from time to time, including as updated on an Order.
- 17.3.1 Any notice or other communication shall be deemed to have been duly received if delivered personally, when left at the address referred to above or, if sent by pre-paid first-class post or recorded delivery, at 9.00 am on the second Business Day after posting, if delivered by commercial courier, on the date and at the time that the courier's delivery receipt is signed, or if sent by email, where receipt of the email is confirmed or acknowledged, including by transmission of an automatic electronic read receipt or a manual acknowledgement from the recipient.
- 17.3.2 This clause 17.3 shall not apply to the service of any proceedings or other documents in any legal action.
- 17.4 **Waiver:** A waiver of any right under this Agreement is only effective if it is in writing and shall not be deemed to be a waiver of any subsequent breach or default. No failure or delay by a party in exercising any right or remedy under this Agreement or by law shall constitute a waiver of that or any other right or remedy, nor preclude or restrict its further exercise. No single or partial exercise of such right or remedy shall preclude or restrict the further exercise of that or any other right or remedy.
- 17.4.1 Unless specifically provided otherwise, rights arising under this Agreement are cumulative and do not exclude rights provided by law.
- 17.5 **Severance:** If a court or any other competent authority finds that any provision of this Agreement (or part of any provision) is invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed deleted, and the validity and enforceability of the other provisions of this Agreement shall not be affected.
- 17.5.1 If any invalid, unenforceable or illegal provision of this Agreement would be valid, enforceable, and legal if some part of it were deleted, the provision shall apply with the minimum modification necessary to make it legal, valid and enforceable.
- 17.6 **No partnership:** Nothing in this Agreement is intended to, or shall be deemed to, constitute a partnership or joint venture of any kind between any of the parties, nor constitute any party the agent of another party for any purpose. No party shall have authority to act as agent for, or to bind, the other party in anyway.
- 17.7 **Third parties:** A person who is not a party to this Agreement shall not have any rights under or in connection with it.
- 17.8 **Variation:** Any variation, including the introduction of any additional terms and conditions, to this Agreement, shall only be binding when agreed in writing and signed by both parties.
- 17.9 **Governing law and jurisdiction:** This Agreement, and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or

claims), shall be governed by, and construed in accordance with, English law, and the parties irrevocably submit to the exclusive jurisdiction of the courts of England and Wales.

17.10 This Agreement has been entered into on the date stated at the beginning of it.

SIGNED by [NAME OF DIRECTOR])

for and on behalf of)

4NET TECHNOLOGIES LIMITED)

SIGNED by [NAME OF DIRECTOR])

for and on behalf of)

[CUSTOMER])

SUPPLY SCHEDULE

18. BASIS OF THE SCHEDULE

18.1 The terms of the main body of this Agreement and the terms of this Schedule shall apply to any Order submitted by the Customer to FourNet for the supply of Goods and Software.

19. GENERAL CUSTOMER OBLIGATIONS

19.1 The Customer shall:

19.1.1 ensure that any information it provides is complete and accurate;

19.1.2 co-operate reasonably with FourNet in all matters relating to the Goods and Services;

- 19.1.3 provide FourNet, its employees, agents, consultants and subcontractors, with access to the Customer's premises, office accommodation and other facilities as reasonably required by FourNet;
 - 19.1.4 provide FourNet with such information and materials as FourNet may reasonably require in order to supply the Services, and ensure that such information is accurate in all material respects;
 - 19.1.5 obtain and maintain all necessary consents, licenses, permissions and authorisations that are required for the Services including; consent for any to buildings on entrance to property required from local authorities, landlords or owners; for the installation of FourNet or 3rd party equipment; or for the use of the Services over the Customers Network or at a site;
 - 19.1.6 comply with, and ensure that its Users comply with, all Applicable Law in the receipt and use of the Services;
 - 19.1.7 Adhere and comply with the Compliance Obligations; and
 - 19.1.8 keep and make available to FourNet any operating manuals and CDs containing programs or other data supplied with any of the CPE.
 - 19.1.9 Be responsible for any material damage to or loss of the FourNet Equipment other than due to fair wear and tear.
- 19.2 The Customer shall not use, and shall prevent its agents, representatives, subcontractors, consultants, and employees from using, the Services:
- 19.2.1 in breach of any reasonable instruction given by FourNet to the Customer from time to time;
 - 19.2.2 in contravention of any licence, code of practice, instruction or guideline issued by any regulatory body, or any third party's rights, which applies to this Agreement;
 - 19.2.3 to send, receive, upload, download, use or reuse any information or material or make any calls that are offensive, abusive, indecent, defamatory, obscene, or are intended to deceive or are in breach of confidence, copyright, privacy or any other similar right;
 - 19.2.4 in an unreasonable manner which may result in FourNet, or its suppliers, causing any liability to a third party;
 - 19.2.5 in a manner which may damage FourNet's reputation, or its suppliers' reputation, or the reputation of the Services, or otherwise bring FourNet, its suppliers, or the Services into disrepute;
 - 19.2.6 fraudulently, improperly, immorally or in connection with a criminal offence or in any way that is unlawful; or
 - 19.2.7 in any way FourNet reasonably considers to be, or likely to be, detrimental to the provision of the Services to the Customer or to the provision of any service to any other customer of FourNet.

20. CUSTOMER EQUIPMENT CONNECTED TO THE SERVICE

- 20.1 Save as set out in the Scope of Work, the Customer will be responsible for connecting handsets to the Service following the procedures set out in the Product Handbook.
- 20.2 The Customer agrees that if it connects any equipment to the Service that is not on the list of approved equipment, the performance of the Service may be impacted. FourNet will not be liable for any faults that, in its reasonable opinion, are attributable to unapproved equipment, and the Customer will be liable for the costs associated with the correction of such faults.
- 20.3 Save as set out in the Scope of Work, the Customer will ensure it has adequate and correctly configured routers and switches and sufficient bandwidth to enable use of the Service.

FourNet will not be liable for any faults that, in its reasonable opinion, are attributable to inappropriate or incorrectly configured Customer Equipment including switches and routers, unless they are supported under contract by FourNet, and the Customer will be liable for the costs associated with the correction of such faults.

- 20.4 The Customer will be responsible for deployment of Customer Equipment unless otherwise stated in the Scope of Work.

21. SITE SURVEY

- 21.1 In certain cases, FourNet, or its suppliers, may need to conduct a site survey at the Customer's premises to ensure the suitability of the Customer's site and/or equipment for the use of the Goods, or Services. Such surveys and site visits shall be conducted in accordance with these Conditions, where the survey is carried out by a 3rd party, such as a Carrier these surveys shall incur a charge, payable by the Customer.
- 21.1.1 This includes a Network Readiness Assessment which is a prerequisite for installation services. If the Customer wishes to waive this assessment, FourNet cannot guarantee sufficient connectivity to enable Services.
- 21.2 Following any site survey, FourNet will notify the Customer of any Charges that are required in order for FourNet to provide the Goods, or Services to the Customer and the Customer may decide to either pay the said Charges or cancel the Order in respect of the affected Goods or Services. The Customer shall within 5 Business Days of the date of it being notified of such Charges notify FourNet of its intention to either pay the Charges or cancel the Order, failing which the FourNet may terminate the Order for the affected Goods with immediate effect by giving written notice to the Customer.
- 21.3 If, following any site survey, FourNet is not able to supply any part of the Goods or Services to the Customer, FourNet may terminate the Agreement for such part with immediate effect by giving written notice to the Customer.
- 21.4 In the event, that any part of an Order is terminated pursuant to paragraph 4.2 or paragraph 4.3, FourNet will refund any advance payments made by the Customer to FourNet in respect of the Charges for the terminated part of the Order.

22. SUPPLY OF GOODS AND SERVICES

- 22.1 FourNet warrants to the Customer that the Goods or Services will be provided using reasonable care and skill. FourNet shall use reasonable endeavours to meet the Service Levels.
- 22.2 FourNet will comply with all Applicable Law in the provision of the Goods and Services.
- 22.3 FourNet shall take reasonable precautions to prevent any unauthorised access by third parties to any part of the telecommunications network provided by FourNet (or its subcontractors), but FourNet will not be liable for any loss or damage sustained by the Customer in the event of any unauthorised access.
- 22.4 FourNet shall use reasonable endeavours to meet any dates to perform, but any such dates shall be estimates only and time shall not be of the essence.
- 22.5 FourNet shall use its reasonable endeavours to provide the Services continuously but FourNet does not warrant or guarantee:
- 22.5.1 that the use of the Services shall be uninterrupted, secure or error-free; or
- 22.5.2 the call quality; or
- 22.5.3 that all calls made by the Customer will be accepted by the telecommunications network which is used in the provision of the Services.

- 22.6 Where applicable, the Services will store recorded calls for 30 days after which the Customer will be responsible for providing and managing storage for call recordings. Alternatively, additional storage may be purchased from FourNet.
- 22.7 Details of approved handsets for use with the Services are available on request.
- 22.8 The Customer will be responsible for providing approved Customer Equipment.
- 22.9 FourNet will be responsible for remotely updating, ensuring compatibility, and maintaining the configuration for all approved Customer Equipment used in association with the Services.

23. QUANTITY AND DESCRIPTION

- 23.1 The quantity and description of the Goods and Software shall be as set out in the Order.
- 23.2 FourNet reserves the right (but does not assume the obligation) to make any change in any specification of the Goods, Software or Services which is required to conform with any applicable legislation, or which does not materially affect the quality or performance of the Goods, Software or Services.

24. MANUFACTURER SOFTWARE

- 24.1 The Customer will comply with the provisions of any Software licences provided with or as part of the Services.
- 24.2 If any Manufacturer Software (or portion of it) provided under this Agreement is installed or downloaded at the Customer premises or on any of the Customer's devices or otherwise made available or accessible to the Customer, the Customer hereby agrees to and shall comply with Manufacturers End User License Agreement ("EULA") for the applicable Software.

25. TITLE AND RISK

- 25.1 The risk in the Goods shall pass to the Customer on completion of delivery.
- 25.2 Until title to the Goods has passed to the Customer, the Customer shall:
 - 25.2.1 hold the Goods on a fiduciary basis as FourNet's bailee;
 - 25.2.2 store the Goods separately from all other held by the Customer so that they remain readily identifiable as FourNet's property;
 - 25.2.3 not remove, deface or obscure any identifying mark or packaging on or relating to the Goods;
 - 25.2.4 maintain the Goods in satisfactory condition and keep them insured against all risks for their full price from the date of delivery;
 - 25.2.5 notify FourNet immediately if it becomes subject to any of the events listed in clause 13.1 of the agreement above; and
 - 25.2.6 give FourNet such information relating to the Goods as FourNet may require from time to time.
- 25.3 Title to the Goods shall not pass to the Customer until FourNet has received payment in full (in cash or cleared funds) for the Goods.
- 25.4 If before title to the Goods passes to the Customer the Customer becomes subject to any of the events listed in clause 13.1, or FourNet reasonably believes that any such event is about to happen and notifies the Customer accordingly, then, provided that the Goods have not been resold, or irrevocably incorporated into another product, and without limiting any other

right or remedy FourNet may have, FourNet may at any time require the Customer to deliver up the Goods and, if the Customer fails to do so promptly, enter any premises of the Customer or of any third party where the Goods are stored in order to recover them.

25.5 Where the Customer procures under this Agreement a Cloud or Rental Service, neither title or risk shall pass to the Customer.

On termination of this Agreement for any reason FourNet's rights in this paragraph 8 shall remain in full effect.

26. WEEE REGULATIONS

26.1 The Customer will:

- 26.1.1 be responsible under Regulation 9 of the Waste Electrical and Electronic Equipment Regulations 2006 ("the WEEE Regulations") for the costs of collection, treatment, recovery, recycling and environmentally sound disposal of any equipment supplied under the Order that has become waste electrical and electronic equipment ("WEEE"). FourNet and the Customer acknowledge that for the purposes of Regulation 9 this Clause is an agreement stipulating other financing arrangements for the collection, treatment, recovery, recycling and environmentally sound disposal of WEEE;
- 26.1.2 be responsible for any information recording or reporting obligations imposed by the WEEE Regulations.

27. CPE

27.1 Title in the CPE shall at all times remain with either FourNet or its suppliers (as the case may be).

27.2 In respect of any CPE supplied to the Customer under the Agreement, the Customer shall:

- 27.2.1 use the CPE in accordance with any instructions FourNet may provide from time to time and only for the purposes of using the Services in accordance with the Agreement;
- 27.2.2 not move, modify, relocate or any way interfere with the CPE;
- 27.2.3 not have the CPE repaired or serviced except by FourNet or any suppliers approved by FourNet in writing;
- 27.2.4 keep the CPE fully insured for risk of loss, theft, destruction, damage;
- 27.2.5 not create or allow any charges, liens, pledges, or other encumbrances to be created over the CPE; and
- 27.2.6 permit FourNet, or its suppliers, to inspect and test the CPE at all reasonable times

27.3 The Customer shall be liable for any damage to the CPE, and FourNet's suppliers' networks, which is caused by the Customer.

28. TELEPHONE NUMBERS

28.1 The Customer will not own any telephone number allocated to it, nor will it have the right to sell or transfer any telephone number to any third party without the prior written consent of FourNet.

28.2 Where the Customer is using an existing telephone number, and that number is not connected to FourNet's network, FourNet may need to perform additional migration work. The Customer undertakes to provide FourNet with any information it may require to carry out

the migration and accepts that the migration may delay the commencement of the Services. FourNet shall have no responsibility for any delays in the commencement of the Services due to the migration unless such delay arises from an act or omission of FourNet.

- 28.3 FourNet reserves the right to change a telephone number allocated to the Customer if FourNet's contract with the third party provider of the telephone number terminates or FourNet's third party provider changes that telephone number.

29. NUMBER ALLOCATION AND PRESENTATION NUMBERS

- 29.1 Where applicable, geographic numbers will be allocated to the Customer by FourNet.
- 29.2 The Customer will be allocated blocks of up to 100 concurrent numbers in a single order.
- 29.3 FourNet may revoke any newly allocated number range on reasonable notice where the Customer is not, in FourNet's reasonable opinion actively making use of such numbers.
- 29.4 FourNet will not be responsible for verifying any information relating to third party or other network operator telephone numbers used as Presentation Numbers.

30. NUMBER PORTING

- 30.1 In line with the Order, FourNet will manage the porting of all numbers to be used in connection with the Service.
- 30.2 There may be some restrictions to number portability.
- 30.3 FourNet will manage the porting of telephone numbers using the information supplied by the Customer in accordance with all relevant legislation and regulations (including codes of practice). It is the Customer's responsibility to secure the co-operation of the losing Communications Provider in any number porting activity requested by the Customer.

31. CALLS

- 31.1 Details of Call types not supported by the Services are available upon request.
- 31.2 If Calls conveyed via the Services for onward termination to an International Destination Network are abnormally high FourNet or the overseas network operator may instigate network management control measures, provided the control measures instigated are reasonably proportionate to the security risk caused. FourNet will notify the Customer of the action taken as soon as is reasonably practicable, provided that in the case of action taken by the overseas network operator, FourNet is made aware of the measures taken.

32. SIP SERVICES

- 32.1 The SIP Services will only become active after satisfactory testing.
- 32.2 The Customer acknowledges that the SIP Services are supplied as a private service for use for certain specific applications which, as regards public emergency call services, confer only limited service at agreed defined locations and is not sold as a full public service. The Customer agrees that FourNet shall be entitled to provide its supplier in respect of each network termination point full details of the Customer's name and address to enable FourNet's supplier to fulfil its obligations to Ofcom.
- 32.3 FourNet does not issue the IP address to be used with the SIP Services. FourNet reserves the right to withdraw or change this IP address if for any reason the address ceases to be available.

- 32.4 The point of connection for the IP connect service is the IP address in the public internet which will be notified by FourNet or its supplier to the Customer. FourNet's responsibility does not extend to the transport between this point and the Customer or to any equipment in operation beyond this point, both of which shall be the responsibility of the Customer. The point of connection for the IP connect service is the pre-configured router to be provided by FourNet or its supplier to the Customer. FourNet's responsibility does not extend to any equipment beyond this router, any or all of which shall be the responsibility of the Customer.

33. CONTENT

- 33.1 Where the Customer provides content for use in connection with the Services ("Content"), the Customer warrants that it has obtained in writing all necessary rights, clearances, and permissions to allow it to use the Content including but not limited to any associated copying, storage, streaming or playing of the Content.
- 33.2 The Customer will obtain any necessary licences from the Performing Right Society (PRS), Mechanical Copyright Protection Society (MCPS), Phonographic Performance Limited (PPL) or any other copyright holder and pay any applicable royalties or other charges to use any Content with the Cloud Service.
- 33.3 If the Customer provided Content is the subject of a claim of infringement of any Intellectual Property Rights or breach of any licensing requirement or if FourNet reasonably believes that the Content is likely to become the subject of such a claim, FourNet may, without notice, delete the Content and /or disable the streaming or playing of the Content.
- 33.4 The Customer will indemnify FourNet against any claims or legal proceedings that are brought or threatened against FourNet by a third party arising from any breach of paragraphs 16.1 or 16.2. FourNet will notify the Customer of any such claims or proceedings and keep the Customer informed as to the progress of such claims or proceedings.

34. IP ADDRESSES, DOMAIN NAMES AND TELEPHONE NUMBERS

- 34.1 Except for IP Addresses expressly registered in the Customer's name, all IP Addresses and Domain Names made available with the Services will at all times remain the property of FourNet or its suppliers and will be non-transferable. All the Customer's rights to use such IP Addresses and/or Domain Names will cease on termination or expiration of the relevant Service.
- 34.2 FourNet cannot ensure that any requested Domain Name will be available from or approved for use by the Internet Registration Authorities and FourNet has no liability for any failure in the Domain Name registration, transfer or renewal process.
- 34.3 The Customer warrants that it is the owner of or is authorised by the owner of the trademark or name that it wishes to use as a Domain Name.
- 34.4 The Customer is responsible for all fees associated with registration and maintenance of its Domain Name and will reimburse FourNet for any and all fees paid by FourNet to any Internet Registration Authorities, and thereafter be responsible for paying such fees directly to the relevant Internet Registration Authorities.
- 34.5 Telephone numbers made available with the Cloud Service will at all times remain the property of FourNet and its subcontractors and will be non-transferable, and the Customer's rights to use telephone numbers will cease on termination or expiration of the Service.

35. DELIVERY

- 35.1 FourNet shall deliver the Goods and/or Software to the Delivery Location at a time agreed between the Parties. Where the Delivery Location is unavailable FourNet will hold the Goods and/or Software until the Delivery Location becomes available

- 35.2 The Customer shall accept delivery of the Goods and/or Software at the Delivery Location on the agreed delivery date.
- 35.3 Delivery of the Goods and/or Software shall be completed on the Goods' and/or Software's arrival at the Delivery Location or, if unavailable, the time FourNet notifies the Customer that the Goods are ready for delivery.
- 35.4 Any dates quoted for delivery are approximate only, and the time of delivery is not of the essence.
- 35.5 The Customer will inspect the Goods on delivery and notify FourNet in writing within 5 Business Days of delivery of any defect in the Goods provided that if no such notification is given it shall be conclusively presumed that the Goods are complete and in good order and condition. Where the Delivery Location is a FourNet location, FourNet will allow the customer to view the Goods at a convenient time for both parties.
- 35.6 FourNet may deliver the Goods by instalments, which shall be invoiced and paid for separately.

36. WARRANTY

- 36.1 Where FourNet is not the manufacturer of the Goods, FourNet shall use reasonable endeavours to transfer to the Customer the benefit of any warranty or guarantee given by the manufacturer to FourNet.
- 36.2 FourNet warrants that on delivery, and for a period of 3 months from the date of delivery ("warranty period"), the Goods shall conform in all material respects with any applicable Specification.
- 36.3 Subject to paragraph 19.4, if:
- 36.3.1 the Customer gives notice in writing to FourNet during the warranty period within a reasonable time of discovery that any of the Goods does not comply with the warranty set out in paragraph 19.2; and
- 36.4 FourNet is given a reasonable opportunity of examining such Goods; and
- 36.4.1 the Customer (if asked to do so by FourNet) returns such Goods to FourNet's place of business;
- at the Customer's cost, FourNet shall, at its option, repair or replace the defective Goods, or refund the price of the defective Goods in full.
- 36.5 FourNet shall not be liable for Goods' failure to comply with the warranty set out in paragraph 19.2 if:
- 36.5.1 the Customer makes any further use of such Goods after giving notice in accordance with paragraph 19.3; or
 - 36.5.2 the defect arises because the Customer failed to follow FourNet's or manufacturer's oral or written instructions as to the storage, commissioning, installation, use and maintenance of the Goods or (if there are none) good trade practice; or
 - 36.5.3 the Customer alters or repairs such Goods without the written consent of FourNet; or
 - 36.5.4 the defect arises as a result of fair wear and tear, wilful damage, negligence, or abnormal storage or working conditions.
- 36.6 Except as provided in this paragraph 19, FourNet shall have no liability to the Customer in respect of the Goods' failure to comply with the warranty set out in paragraph 19.
- 36.7 Except as set out in this Agreement, all warranties, conditions and other terms implied by statute or common law are, to the fullest extent permitted by law, excluded from this Agreement.
- 36.8 This Schedule shall apply to any repaired or replacement Goods supplied by FourNet.

37. SECURITY

- 37.1 The Customer acknowledges that use of VoIP, like other network-based services, carries certain security risks to the systems and networks of customers, network providers and third parties including, but not limited to: misuse; unauthorised access; alterations; theft; fraud; destruction; corruption; and attacks ("Occurrences"). The Customer will ensure that it takes security measures including but not limited to the use of firewalls, passwords, access restrictions, encryption, policies, and physical access restrictions to protect from Occurrences all VoIP traffic, equipment, software, data, and systems located on the Customer's premises or otherwise in the Customer's control and used in connection with VoIP, whether owned by the Customer, FourNet, or FourNet's subcontractors.

38. SUSPENSION

- 38.1 Without limiting its other rights or remedies, FourNet shall have the right to suspend provision of the Services if:

38.1.1 FourNet reasonably believes that the Services are being used in an unauthorised or illegal manner; or

38.1.2 Ofcom or any other regulatory body requires FourNet to suspend the Services;

38.1.3 to conduct Planned Maintenance, in which case FourNet will notify the Customer in advance;

38.1.4 if FourNet (or its subcontractors) reasonably considers that it is required to do so in order to safeguard the integrity and security of its network.

- 38.2 FourNet will endeavour to notify the Customer in advance of any restriction or suspension for any of the events listed in paragraph 21.1 as soon as commercially reasonable.

- 38.3 Where FourNet exercises its rights to restrict or suspend the Service in paragraph 21.1.4 where the need to safeguard the integrity of security of the network arose as a result of a breach by the Customer:

38.3.1 the Customer will continue to be liable for all applicable Charges for that Service until the Order is terminated; and

- 38.4 FourNet may charge a re-installation fee in order to resume supply of the Cloud Service to the Customer. FourNet reserves the right to suspend and/or withdraw the use of the Presentation Numbers without notice if:

38.4.1 it is subsequently found that the information supplied by the Customer was, or has become, inaccurate; and/or

38.4.2 FourNet reasonably believes that a Presentation Number is being used:

(i) in a way prohibited by the CLI Code of Practice; and/or

(ii) to generate revenue-sharing

- 38.5 FourNet will process orders for Type 3 and Type 5 Presentation Numbers based upon the information supplied by the Customer on the CRF.

39. EXCUSED PERFORMANCE

- 39.1 FourNet will not be in breach of the Order, nor legally liable, for any failure or delay to perform any of its obligations under the Order (including any of its obligations to meet the Service Levels, if any) if and to the extent that FourNet's failure or delay in performing arises as a result of:

- 39.1.1 Any failure or delay by the Customer to perform any of the Customer's obligations under the Order (Customer Default)
 - 39.1.2 Any act or omission other than on the part of FourNet or a subcontractor appointed by it; or
 - 39.1.3 A Regulatory Body restricting or preventing FourNet (or a subcontractor) from supplying the Cloud Service.
- 39.2 The Customer shall reimburse FourNet on written demand for any reasonable costs, charges, or losses sustained or incurred by FourNet arising directly or indirectly from the Customer Default.

ANNEX 1 to Supply Schedule

3RD PARTY SUPPLIER END USER LICENCE TERMS

The 3rd Party Supplier END USERS LICENCE TERMS will be sent separately and updated from time to time.

SERVICES SCHEDULE

40. BASIS OF SCHEDULE

- 40.1 The terms of the main body of this Agreement and the terms of this Schedule shall apply to the supply of Services by FourNet to the customer.

41. IMPLEMENTATION SERVICES

- 41.1 Installation Services will be undertaken by accredited personal who will install and configure hardware and software as laid out in the Order and the Statement of Works.
- 41.2 Project Co-Ordination provides remote basic project management and support to the project manager as set out in the Order and the Statement of Works.

- 41.2.1 Project Management will meet the requirements and responsibilities as set out in the Order and the Statement of Works.
- 41.2.2 Consultancy services will be described in the Order and the Statement of Works.
- 41.3 Training services will be set out in the Order and the Statement of Works.

IMPLEMENTATION LIMITATIONS

- 41.4 2.4If FourNet's performance of any of its obligations under this Agreement is prevented or delayed by any act or omission by the Customer or failure by the Customer to perform any relevant obligation (Customer Default):
 - 41.4.1 FourNet shall be relieved from the performance of any of its obligations to the extent the Customer Default prevents or delays FourNet's performance of any of its obligations; and
 - 41.4.2 the Customer shall reimburse FourNet on written demand for any costs, charges or losses sustained or incurred by FourNet arising directly or indirectly from the Customer Default.
- 41.5 FourNet have not included any UPS unless stated in the Order.
- 41.6 Unless otherwise stated in the Order, the Services do not include the unpacking, building, deployment, wall-mounting, patching or testing of handsets.
- 41.7 Decommissioning or de-installation, and removal of old hardware is not included in the Service.
- 41.8 Software and licensing shall only be deployed and installed where explicitly stated in the Order.
- 41.9 Any customer deliverables which are not met or completed prior to engineering site visits may be subject to change control and may result in Additional Charges for resource time.
- 41.10 Any changes to the approved Scope of Works will be subject to project change control and may result in Additional Charges.
- 41.11 FourNet will undertake implementation work during Business Hours unless otherwise stated in the Order.
- 41.12 Unless otherwise agreed, FourNet will not be responsible for organising, liaising with or managing third parties who are not directly employed to carry out the implementation by FourNet.
- 41.13 The lead time for Ethernet circuits is between 60 and 90 days, subject to survey.

ACCEPTANCE TESTS

- 41.14 FourNet shall notify the Customer when the Service is ready for delivery. Following receipt of such notice, the Customer will promptly carry out the agreed Acceptance Tests for the Service. FourNet will not be liable to meet any Service Levels or to pay any Service Credits (if Service Credits are payable) if the Customer has not:
 - 41.14.1 carried out the Acceptance Tests and confirmed acceptance in writing to FourNet; or
 - 41.14.2 notified FourNet in writing that the Service has not passed the Acceptance Tests.

42. CUSTOMER IMPLEMENTATION RESPONSIBILITIES

- 42.1 The Customer must monitor and maintain any Customer Equipment connected to the Service or used in connection with the Service;

- 42.2 The Customer must ensure that any Customer Equipment used directly or indirectly by the Customer or User with the Service is:
- 42.2.1 used in accordance with any instructions, standards and safety and security procedures applicable to the use of that Customer Equipment;
 - 42.2.2 approved and used in accordance with relevant instructions and Applicable Law;
 - 42.2.3 immediately disconnect any Customer Equipment, or advise FourNet to do so at the Customer's expense, if Customer Equipment does not meet any relevant instructions, standards or Applicable Law;
 - 42.2.4 at a reasonable time agreed by FourNet and to enable FourNet to carry out its obligations under this Agreement, use its reasonable endeavours to provide, FourNet employees and anyone acting on FourNet's behalf who produces a valid identity card, access to any Site. FourNet will normally only require access during the Working Day but may, on reasonable notice, require the Customer to provide access at other times. FourNet may agree to work outside the Working Day but the Customer will pay FourNet's Additional Charges, as advised to the Customer prior to the Additional Charges being incurred;
- 42.3 The Customer will maintain a list of current Administrators and Users and immediately terminate access for any person who ceases to be an authorised Administrator or User;
- 42.4 The Customer will ensure the security and proper use of all valid Administrator and User access profiles, passwords and other system administration information used in connection with the Service and:
- 42.4.1 inform FourNet as soon as reasonably practicable if a user identification ("ID") or password has, or is likely to, become known to an unauthorised person, or is being or may be used in an unauthorised way;
 - 42.4.2 take all reasonable steps to prevent unauthorised access to the Service;
 - 42.4.3 satisfy FourNet's security checks if a password is lost or forgotten;
 - 42.4.4
 - 42.4.5 if reasonably requested to do so by FourNet in order to ensure the security or integrity of the Service, or as a result of a security breach, change any or all passwords and/or other system administration information used in connection with the Service;
- 42.5 The Customer will take all reasonable steps (including testing with the latest commercially available virus detection software) to ensure that any software used with or in conjunction with the Service is not infected by viruses and/or logic bombs, worms, trojan horses and any other type of disruptive, destructive or nuisance programs;
- 42.6 The Customer will not exploit a Presentation Number to generate revenue-sharing calls. Such exploitation may constitute persistent misuse of an Electronic Communications Network or Electronic Communications Service and FourNet may suspend the Service and/or terminate the Order in such circumstances;
- 42.7 The Customer will, unless otherwise agreed with FourNet, add or delete Users for any Application at any time system administration Portals;
- 42.8 Unless otherwise agreed with FourNet, the Customer will manage User level MACDs and configuration changes via the system administration Portals:
- 42.8.1 provide FourNet with a minimum of 72 hours' notice of any planned changes in the Customer's network environment that may impact the Service;
 - 42.8.2 immediately inform FourNet in writing of any changes to the information the Customer supplied when registering for the Service;
 - 42.8.3 unless otherwise agreed with FourNet, be responsible for adding or deleting Users for any Application at any time via the system administration Portals;

- 42.8.4 unless otherwise agreed with FourNet, be responsible for managing User level MACDs and configuration changes via the system administration Portals;
- 42.8.5 ensure that all porting requests contain clear and accurate information. Failure to do so may result in extended lead times and Additional Charges being raised.
- 42.9 The Customer must provide local on-premise all environmental requirements including power, power cords if these are required to be different to those supplied by FourNet (standard UK&I 3-pin), UPS, rack-space and temperature control if identified during the design stage of the project.
- 42.10 During the data capture of technical and functional system information details, Customer assistance must be provided to capture, document and sign off on details such as IP addressing schema, remote access requirements and station configuration through to dial plan and network carrier trunking.
- 42.11 All network configuration must be configured in advance of installation as required by the Supplier.
- 42.12 The Customer must provide a layout plan for phones showing desks and other locations as required by the Supplier.
- 42.13 Provision of local on-premise patch cabling from structured cabling outlets around the building to user and other desk locations must be available.
- 42.14 The Customer should designate a single point of contact, who has a thorough understanding of the business requirements and technical environment, and who will be authorised to make binding decisions.
- 42.15 The Customer must provide support personnel to assist with the provision of local on-premise LAN as identified during the design stage of the project.
- 42.16 The Customer must ensure all staff are briefed on the Supplier requirements and their responsibilities during the project.
 - 42.16.1 The Data Network must be ready for Voice which includes:
 - 42.16.2 A configured voice VLAN and QOS implemented to prioritise voice traffic.
 - 42.16.3 The provision of Power over Ethernet (PoE) for IP phones.
 - 42.16.4 The provision and configuration of network routers.
 - 42.16.5 The DHCP configuration for IP Phones.
- 42.17 Criteria for User Acceptance Testing must be documented by the Customer and shared with the Supplier prior to Testing.
- 42.18 The Customer is responsible for the completion of User Acceptance Testing, by agreement that the solution has met Acceptance Criteria, the Customer agrees that the solution is ready to go live as a fully tested and operationally sound system according to the Customer requirements.
- 42.19 The Customer will be required to approve and authorise documentation throughout the project to ensure the availability of resources and agreement of project details.
- 42.20 The Supplier requires internet connection to be available during visits to Customer locations.
- 42.21 The Customer will provide IP network resource to be available during all phases of the implementation.

43. FOURNET RESPONSIBILITIES

- 43.1 Before the Service Delivery Date and, where applicable, throughout the provision of the Services, FourNet will:

- 43.1.1 comply with all reasonable health and safety rules and regulations and reasonable security requirements that apply at a Site and are notified to FourNet in writing. FourNet will not be liable to the Customer if, as a result of any such compliance, FourNet is in breach of any of its obligations under this Agreement;
- 43.1.2 provide the Customer with a date on which delivery of the Services (or each part of the Services) is due to start and will use its reasonable endeavours to meet any date;
- 43.1.3 use its reasonable endeavours to provision the Services by any date agreed with the Customer but will have no liability for a failure to do so;
- 43.1.4 provide to the Customer copies of (or provide access to if held on a web interface) the documentation necessary for the Customer to access and use the Service as contemplated by this Agreement;
- 43.1.5 ensure that any information it provides is complete and accurate;
- 43.1.6 comply with, and ensure that it complies with, all Applicable Law in relation to the Services;
- 43.1.7 obtain and maintain all necessary licences, permissions and consents which may be required for the receipt of the Services; and
- 43.1.8 keep and make available to FourNet any operating manuals and CDs containing programs or other data supplied with any of the Equipment.

44. MANAGED SERVICES AND CLOUD SERVICES

- 44.1 FourNet will provide to the Customer Managed Services as set out in the Order.
- 44.2 The Customer will have the following components in place to connect to the Services in order for the Services to function and will ensure that these components meet the minimum technical requirements specified by FourNet:
 - 44.2.1 where not provided by FourNet, an appropriate access network and any corresponding data hardware (e.g. router, port switches) to support VoIP with sufficient bandwidth to meet the Customer requirements and their interface to the Services, as set out in the Scope of Works;
 - 44.2.2 appropriate Local Area Network infrastructure plus any corresponding router or port switches suitable to deliver the Customer requirements to Agents and Users;
 - 44.2.3 personal computers or laptops meeting the minimum requirements as notified by FourNet;
 - 44.2.4 internet browser meeting the minimum Service requirements as notified by FourNet; and
 - 44.2.5 inbound Services supplied and configured to support any non-geographical numbers (each an "Enabling Service").
 - 44.2.6 A sufficiently secure and stable remote access method to enable FourNet to deliver support in the event of an Incident, available continually. Where this is not available, FourNet will not be responsible for delays to the delivery of service restoration.
- 44.3 Before the Service Delivery Date and, where applicable, throughout the provision of the Service by FourNet, the Customer will:
 - 44.3.1 provide FourNet with the name(s) and contact details of the individual(s) authorised to act on behalf of the Customer for Service management matters ("Customer Contact"), but FourNet may also accept instructions from a person who FourNet reasonably believes is acting with the Customer's authority;

- 44.3.2 provide FourNet with any information reasonably required without undue delay;
 - 44.3.3 respond to reasonable queries from FourNet without undue delay;
 - 44.3.4 ensure that its LAN protocols and Customer Equipment are compatible with the Service;
 - 44.3.5 provide and maintain a VOIP enabled access network which provides full end to end Quality of Service and sufficient uncontested bandwidth to support the Services at the Site(s) for use with the Services as notified by FourNet;
 - 44.3.6 pay all charges related to provision and use of the VOIP enabled access network and report any incidents in the network directly to the supplier of it.
- 44.4 The Customer warrants that any software provided as part of any Customer Equipment it presents for integration with the Service:
- 44.4.1 is written in an appropriate manner such that its security and overall system performance is preserved; and
 - 44.4.2 complies with any applicable code of practice FourNet makes available to the Customer;
- 44.5 For Number Allocation, the Customer will provide FourNet with information regarding the utilisation of allocated numbers as reasonably requested by FourNet.
- 44.6 For Presentation Numbers, the Customer undertakes and warrants that, if it intends to use Type 3 and Type 5 Presentation Number:
- 44.6.1 permission is not required from anyone else in relation to the numbers; or
 - 44.6.2 if the Presentation Numbers are not allocated to the Customer, it provides to FourNet evidence of written consent from the allocated owner for its use as a Presentation Number; and
 - 44.6.3 advises FourNet immediately if that consent is withdrawn;
 - 44.6.4 the Presentation Numbers used are dialable numbers or are numbers that have been received from the PSTN and passed on unchanged in accordance with the terms of the CLI Code of Practice;
 - 44.6.5 to inform FourNet immediately of any changes in relation to 5.6.1 to 5.6.4 above; and
 - 44.6.6 the Presentation Number will not be:
 - (i) a Premium Rate Service number (as defined in Section 120 of the Telecommunications Act of 2003) prefixed 09; or
 - (ii) a number that connects to a revenue sharing number that generates an excessive or unexpected Call Charge.
 - 44.6.7 it will comply with the CLI Code of Practice.
- 44.7 For Number Allocation, the Customer will provide FourNet with information regarding the utilisation of allocated numbers as reasonably requested by FourNet.
- 44.8 The Customer will indemnify and hold FourNet harmless against all claims, losses, costs and liabilities arising from its failure to comply with paragraph 5.6.
- 44.9 The Customer will access the Service via a secure private network access. FourNet will not be liable for any security breach as a result of the Customers failure to comply with this paragraph 5.9.

45. FOURNET SERVICE DESK

45.1 The FourNet Service Desk provides support to the customer in line with the SLA set out in the Order. Incidents can be logged via the Customer Portal, Email or Telephone. The service desk is structured as follows:

45.2 First Line Support and Incident Management:

45.2.1 The First Line team are responsible for taking and logging Incidents and to provide an in-depth triage service. They will then pass the Incident to the relevant Resolver Group; the team also proactively manage the Resolver Groups to ensure optimum restoration times. Major Incidents (P1, P2) will be assigned a Major Incident Manager to act as a single point of contact for the Customer and to manage all parties involved in the restoration of service.

45.3 Second Line Support:

45.3.1 Second Line are the Resolver Groups for Incidents of all Priority Levels and will actively work with the Customer and the Software Provider to resolve Incidents as quickly as possible. They are also responsible for carrying out proactive maintenance and monitoring services to ensure events are resolved before they become Incidents. This team also provides onsite support services and part replacement where deemed necessary.

45.4 Third Line Support:

45.4.1 Third Line offer support to the Second Line Resolver Groups and will manage manufacturer escalations. Third Line work closely with the management team to ensure Incident trends are monitored to ensure optimum solution uptime is achieved.

45.5 Where set out in the Order FourNet will provide a Service Delivery Manager to the Customer. The Service Delivery Manager provides proactive management of the service and provides analytical data to measure service performance. The Service Delivery Manager is an escalation point for the customer and will work to ensure the service continually develops and improves throughout the Term.

45.6 Escalation Management:

45.6.1 The Service Desk Team Leaders, Managers and ultimately the Services Director provide an escalation point for the Service Desk and the Customer. The Management team provide support to the team and will look to proactively manage the service to ensure restoration times perform in line with the defined SLA as set out in the Order and ensure preventive measures are carried out in order to avoid incidents.

45.7 The Customer Portal gives the Customer access to log Incidents and check for progress on Incidents via a web browser.

46. SERVICE MANAGEMENT BOUNDARY

46.1 FourNet will provide and manage the Managed Services up to and including the FourNet provided access Circuits and associated termination hardware ("Service Management Boundary"). The Service Management Boundary is set out in the Operating Services Manual, The Statement of Works and/or the Order.

46.2 FourNet will have no responsibility for the Services outside the Service Management Boundary.

46.3 Customer specific physical and logical access circuits not provided by FourNet will be outside the Service Management Boundary. In this instance, the Service Management Boundary will be the physical interface between the FourNet network, and the Customer provided circuits.

47. NOTIFICATION OF INCIDENTS

- 47.1 FourNet will only be responsible for rectifying faults that lie within the Service Management Boundary and will not be responsible for rectifying faults with the Customer's network, third party software or Customer Equipment unless supplied by FourNet under the Order.
- 47.2 Where the Customer becomes aware of an Incident and reasonably believes that the Incident relates to the Managed Service:
- 47.3 the Customer Contact or Customer's internal helpdesk will report it to FourNet;
- 47.3.1 FourNet will give the Customer a unique reference number for the Incident
- 47.3.2 FourNet will inform the Customer when it believes the Incident is cleared.
- 47.3.3 FourNet will pause the timing measurements for the SLA in the event that the Customer is required to provide further information regarding the Incident.
- 47.4 FourNet will close the Incident when:
- 47.4.1 the Customer confirms that the Incident is resolved within 24 hours of being informed; or
- 47.4.2 FourNet has attempted unsuccessfully to contact the Customer, in the manner agreed between the Customer and FourNet, in relation to the Incident and the Customer has not responded within 24 hours of FourNet's attempt to contact.
- 47.5 If the Customer advised FourNet that the Incident is not resolved within 24 hours of being informed that the Incident has been cleared, the Incident will remain open, and FourNet will continue to endeavour to resolve the Incident and, where appropriate, Availability downtime will continue to be measured by FourNet, until the Incident is closed in accordance with paragraph 8.4
- 47.6 FourNet will not accept Incident notifications from Users other than the Customer Contact or the Customer's internal helpdesk.

48. ACCESS TO APPLICATIONS

- 48.1 The Applications available within the Goods or Services are available from FourNet upon request and subject to update from time to time.
- 48.2 FourNet will provide all Applications in English and all the user interfaces and reports will be labelled in English.
- 48.3 The Managed Service supports the integration of Customer or 3rd party owned applications via the application programming interfaces (APIs) where specifically defined in the Order. Where such integration is part of the solution specific terms relating to support will be defined in the Order.

49. MANUFACTURER SUPPORT

- 49.1 Where defined on the Order, FourNet will escalate incidents to Software and Hardware manufacturers and manage incidents through to resolution.

50. PARTS REPLACEMENT

- 50.1 Where defined in the Order FourNet will replace faulty Equipment,
- 50.2 FourNet may supply reconditioned replacement parts where, in the opinion of FourNet, any parts of the Equipment require replacement. Once such replacement parts have been installed, those parts shall become the property of the Customer.
- 50.3 Any parts replaced by FourNet shall upon removal become the property of FourNet and the Customer warrants that FourNet shall have free and unencumbered title to the same.

50.4 Where the Customers, and as defined in the Order, opts to provide First Line and/or Second line support, FourNet will ship parts to site for replacement by the Customer under remote support from the FourNet service desk.

50.5 Where FourNet is not able to reasonably source replacement Equipment, FourNet shall be under no responsibility to replace the same.

51. PERFORMANCE MANAGEMENT

51.1 Where defined in the Order FourNet will provide a Proactive Monitoring Service for the Services.

51.2 Monitored components will be defined in liaison with the Customer and detailed in the Operations Service Manual, The Statement of Works and/or the Order.

51.2.1 Service Availability will be calculated as below:

51.2.2 Monthly Availability performance (%) = $(A - B - C) / (A - C) \times 100\%$

51.2.3 where: A = total number of minutes in a month B = total number of minutes the individual service has been Out of Service during a month C = Scheduled Maintenance time or Planned Downtime.

52. SCHEDULED AND UNSCHEDULED OUTAGES

52.1 For the purpose of updating facilities, and Planned Maintenance, scheduled downtime may occur from time to time. FourNet:

52.1.1 will use its reasonable endeavours to provide the Customer with advance notice of any scheduled downtime;

52.1.2 will use its reasonable endeavours to keep all scheduled downtime to the quietest time on the Service;

52.1.3 may occasionally suspend the Services for operational reasons (such as maintenance or service upgrades) or because of an Emergency, but before doing so will give the Customer as much notice as reasonably possible and whenever practicable will agree with the Customer, when the Services will be suspended.

53. MANAGED SERVICE OPTIONS

53.1 FourNet will provide to the Customer any of the following options that are set out in any applicable Order and in accordance with the details set out in that Order:

53.1.1 Maintain

Included Services;
Access to FourNet Service Desk
Remote Software Support
Remote System Access via Access Concentrator
Parts Replacement, as defined in Paragraph 2.8
Tier 1 Fault Management
Tier 2 Fault Resolution
Tier 3 Technical Support
Service Desk Management Support
Manufacturer Escalation as defined in Paragraph 3.2.6

53.1.2 Perform

All Services defined in Table 7.2.1 Plus
Named Service Delivery Manager:
Service Performance Reports
Continual Improvement, Service Review and Development
Operational Services Manual (OSM)
Optional Monthly or Quarterly reporting Periods
Performance Management: (as defined in Paragraph 3.2.8)
Proactive System Monitoring
Live Dashboards
Voice Quality Monitoring
Automated Workflow Resolution
System Health Monitoring
Asset Utilization and Capacity Planning

53.1.3 Assure

All Services defined in Table 7.2.2 plus
Software Management:
Firmware Patching
Software Patching
Asset Management:
Automated Configuration Management Data Base (CMDB)
Network Connectivity
Vector Mapping
Change Management:
Audit Logs
Change Scheduler

53.1.4 Protect +

All Services defined in Table 7.2.3 plus
Data Recovery Management
Automated System Configuration Backup
System Recovery
Business Continuity
Security Management
Unauthorized Access Protection
Toll Fraud Management
Security Patching

53.1.5 SUPPORT HOURS

53.1.6 FourNet can provide the service to cover the hours laid out in the table below and the selected option specified in the Order:

Week Day Coverage	
Hours	08:30 to 17:30
Days	Monday to Friday (excluding Bank and Public Holidays)
24 x 7 x 365 Operation	
Hours	24 Hours a Day
Days	7 Days
Tailored Coverage	
Hours	Set out in the Order
Days	Set out in the Order

54. EXCLUSIONS

54.1 The Managed Services do not include services required:

- 54.1.1 as a result of damage to the Equipment caused by the Customer, its employees, its subcontractors or any other person.
- 54.1.2 to be performed outside of Support Hours;
- 54.1.3 where there is no fault with the Equipment, or any fault cannot be replicated;
- 54.1.4 due to the Equipment not being used in accordance with its manufacturer's published instructions;
- 54.1.5 due to the use of parts or supplies not approved by FourNet or the Equipment's manufacturer
- 54.1.6 due to the alteration, modification or repair of the Equipment by a party other than FourNet and its authorised representatives;
- 54.1.7 where the Customer has not carried out procedures or services, recommended by FourNet, to the Equipment;
- 54.1.8 as a result of any physical damage to the Equipment other than through fair wear and tear;
- 54.1.9 relating to any software which is a version no longer supported by the manufacturer or to which the manufacturer charges additional fees for support of the same.

54.2 FourNet shall, following a request for support by the Customer in the circumstances set out in Section 15.1, be entitled to charge the Customer the Additional Charges where FourNet provides Managed Services in respect of the same.

55. THE END OF SERVICE

55.1 On termination of the Order, the Customer will in accordance with FourNet's instructions:

- 55.1.1 Return and/or destroy any Manufacturer Software that does not carry a Perpetual License provided under the Order that has been installed or downloaded at the Customer's premises on any of devices, or otherwise made available or accessible by the Customer, and
- 55.1.2 Provide FourNet with certified compliance by an authorised representative of the Customer that the requirements set out in paragraph 16.1.1 have been met.
- 55.1.3 Return any devices used to deliver the Service which are not owned by the Customer. Any devices not returned will be charged for at the current manufacturers recommended retail price.
- 55.1.4 Where necessary, enable FourNet to default system administrator passwords.

56. INCIDENT PRIORITY LEVELS

The Incident Priority Levels for the Managed Services are as follows:

Priority	Definition
1	Critical Fault The Services are Unavailable across all applications and multiple sites.
2	Non-Critical Fault, High Business Impact The Services are Unavailable across an individual application or one site.
3	Non-Critical Fault The Services are Unavailable to a group of users.
4	Request for Information The Services are Unavailable to an individual user.
5	Moves, Adds, Changes, Deletions (MACD) Request to make a change on the customers system, unless explicitly defined in the Order these requests carry an additional charge.
Where the Customer has opted for 24*7*365 coverage, P1 and P2 Incidents are covered 24 hours a day. P3/P4 and P5 Incidents are managed Monday to Friday 08:30 to 17:30	

57. INCIDENT RESPONSE AND RESTORATION TIMES

Action	Definition	Incident Priority Level Response Targets									
		P1		P2		P3		P4		P5	
A: First Response	FourNet have received and logged the Incident and passed to a Resolver Group	30 Minutes		1 Hour		2 Hours		4 Hours		8 Hours	
B: Second Response	Resolver Group are actively engaged in Incident investigation, logged on to relevant systems and engaged with the Customer.	1 Hour		4 Hours		2 Days		3 Days		5 Days	
C: Target Restoration	FourNet target to have the Incident resolved or a workaround within the defined times.	4 Hours		8 Hours		3 Days		3 Days		5 Days	
First Escalation	Incident Escalated to Tier One team Leader, SDM and Service Desk Manager. A meeting convened and a plan of action defined.	A	22 Mins	A	45 Mins	A	90 Mins	A	90 Mins	A	90 Mins
		B	45 Mins	B	3 Hours	B	12 Hours	B	2 Days	B	3 Days
		C	3 Hours	C	6 Hours	C	2 Days	C	2 Days	C	3 Days
Second Escalation	Incident raised with the Services Director	A	27 Mins	A	54 Mins	A	2 Hours	A	2 Hours	A	2 Hours
		B	54 Mins	B	3.5 Hours	B	14 Hours	B	14 Hours	B	4 Days
		C	3 Hours	C	6 Hours	C	21 Hours	C	14 Hours	C	4 Days

58. THIRD PARTY RESPONSE TIMES

58.1 Where the Services are delivered by a 3rd Party Supplier to FourNet different Response Times may be relevant. Our current Service offerings with Response Times are shown in Appendix 1 and are subject to change.

Appendix 1

BT	Service		High	Medium	Minor	RFI
	Wholesale SIP	Target Response	2 hrs	4 hrs	8 hrs	5 working days
	Wholesale SIP	Target Restoration	4 hrs	8 hrs	24 hrs	N/A
Convergence Group	Internet Access Services		P1	P2	P3	P4
	Diverse Fibre		6 hrs	9 hrs	24 hrs	72 hrs
	Resilient RO2 Fibre		6 hrs	9 hrs	24 hrs	72 hrs
	Resilient RO1 Fibre		6 hrs	9 hrs	24 hrs	72 hrs
	Fibre with Backup		6 hrs	9 hrs	24 hrs	72 hrs
	Fibre		6 hrs	9 hrs	24 hrs	72 hrs
	EFM		8 hrs	12 hrs	24 hrs	72 hrs
	G. Fast / FTTC-GEA		20 hrs	24 hrs	24 hrs	72 hrs
Convergence Group	WAN Services		P1	P2	P3	P4
	Diverse Fibre		5 hrs	8 hrs	24 hrs	72 hrs
	Resilient RO2 Fibre		5 hrs	8 hrs	24 hrs	72 hrs
	Resilient RO1 Fibre		5 hrs	8 hrs	24 hrs	72 hrs
Gamma	Service		P1	P2	P3	P4
	SIP		4 hrs	8 hrs	3 working days	7 working days
	Ethernet Services		6 hrs	1 working day	3 working days	N/A
Virtual One	Service		P1	P2		
	Fibre Ethernet, EFM or EoFTTC	Target Response	30 mins	30 mins		
		Target Restoration	6 hrs	6 hrs		
	ADSL, FTTC Broadband with Enhanced Care	Target Response	30 mins	30 mins		
		Target Restoration	24 hrs	24 hrs		
	ADSL, FTTC Broadband with Standard Care	Target Response	30 mins	30 mins		
		Target Restoration	48 hrs	48 hrs		
	CE	Target Response	30 mins	30 mins		
		Target Restoration	120 hrs	120 hrs		

THE ORDER SCHEDULE

The Order

THIS ORDER SCHEDULE is made on the [DATE].

This Order constitutes an ORDER under this MASTER AGREEMENT dated [] between [CUSTOMER NAME] (the "Customer") and 4Net Technologies Limited (the "Supplier")

Order Charges Summary

Professional Services	
Equipment and Software	
Managed Service/Cloud	
Rentals	
Network Services	

This ORDER SCHEDULE is signed by [CUSTOMER NAME] and 4Net Technologies Limited on the date referred to above.

SIGNED by [NAME OF DIRECTOR])

for and on behalf of)

4NET TECHNOLOGIES LIMITED)

SIGNED by [NAME OF DIRECTOR])

for and on behalf of)

CUSTOMER)

Professional Services

FourNet shall provide the Professional Services detailed below in delivering this Order.

The agreed payment milestone schedule for this Order is:

One Off Charges

Professional Services Delivery Milestones

Implementation Stage	Professional Service Percentage	Approximate Date	Invoice Value
Deposit			
Delivery and Staging			
UAT Commencement			
Training			
Project Sign Off			
TOTAL			

Goods Summary

Description	Invoice Date	Invoice Value
Software/Hardware		
TOTAL		

Professional Services Summary

Professional Service Description	Number of Days	Extended Charges
Project Management/Coordination		
Remote/Onsite Installation		
Training		
Consultancy		
Business Analysis		
TOTAL		

Unless otherwise stated, Professional Services shall take place during Business Hours.

Order Specific Limitations

Insert caveats

Installed Equipment and Software

As described in the table below, the following equipment and licenses shall be installed under this Order.

Description	Quantity	Installation Location

Delivery Location Address (if different to Installation Address):

Managed Service, Cloud and Rentals

The following Service shall be provided under this order from the Service Delivery Date for the Initial Term and Renewal Period thereafter.

Service Delivery Date:

Manufacturer Service Delivery Date:

Initial Term:

Managed Service Level	<i>Maintain/Perform/Assure/Protect Plus</i>
Coverage Hours	<i>Weekday/24x7/Bespoke</i>
Service Delivery Management	<i>Monthly/Quarterly</i>
Solution	<i>Agile Cloud/On-Premise System/Other Cloud/Subscription Service/ Rentals/ Network Service</i>
Invoice Frequency	<i>Monthly/Quarterly/Annually</i>
Invoice Payment Method	<i>BACS/Direct Debit</i>

Charges shall be payable within 30 days of invoice date via the agreed Invoice Payment Method.

Service Description

The following items shall be supported and form the Cloud Service:

Description	Quantity	Consumption Model	Installation Location	Annual Recurring Charge

Order Specific Terms



Information Commissioner's Office

Annex to International Data Transfer Agreement

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Agreement

VERSION A1.0, in force 21 March 2022

This IDTA has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties and signatures

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	<p>Full legal name:</p> <p>Trading name (if different):</p> <p>Main address (if a company registered address):</p> <p>Official registration number (if any) (company number or similar identifier):</p>	<p>Full legal name: APAC Remote Support Limited</p> <p>Trading name (if different): N/A</p> <p>Main address (if a company registered address): 5 Hallwood Road Handforth Cheshire SK9 3BE</p> <p>Official registration number (if any) (company number or similar identifier): 11711826</p>
Key Contact	<p>Full Name (optional):</p> <p>Job Title:</p> <p>Contact details including email:</p>	<p>Full Name (optional): Darren Colker</p> <p>Job Title: Director</p> <p>Contact details including email: darrencolker@apacremotesupport.com</p>

Importer Data Subject Contact		Job Title: Director Contact details including email: darrencolker@apacremotesupport.com
Signatures confirming each Party agrees to be bound by this IDTA	Signed for and on behalf of the Exporter set out above Signed: Date of signature: Full name: Andrew Male Job title: Executive Director of Infrastructure Services	Signed for and on behalf of the Importer set out above Signed: Date of signature: Full name: Darren Colker Job title: Director

Table 2: Transfer Details

UK country's law that governs the IDTA:	<input checked="" type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
Primary place for legal claims to be made by the Parties	<input checked="" type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: <input checked="" type="checkbox"/> Exporter is a Controller <input type="checkbox"/> Exporter is a Processor or Sub-Processor
The status of the Importer	In relation to the Processing of the Transferred Data: <input type="checkbox"/> Importer is a Controller <input checked="" type="checkbox"/> Importer is the Exporter's Processor or Sub-Processor <input type="checkbox"/> Importer is not the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)

Whether UK GDPR applies to the Importer	<input checked="" type="checkbox"/> UK GDPR applies to the Importer's Processing of the Transferred Data <input type="checkbox"/> UK GDPR does not apply to the Importer's Processing of the Transferred Data
Linked Agreement	<p>If the Importer is the Exporter's Processor or Sub-Processor – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data:</p> <p>Name of agreement: Supplier Agreement</p> <p>Date of agreement: 01/12/2020</p> <p>Reference (if any):</p> <div data-bbox="564 712 616 770" data-label="Image"> </div> <p>20201028_Fournet Supplier Agreement_4</p> <p>Parties to the agreement: APAC Remote Support Limited and FourNet Technologies Limited</p> <p>Other agreements – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement:</p> <p>Name of agreement: N/A</p> <p>Date of agreement: N/A</p> <p>Parties to the agreement: N/A</p> <p>Reference (if any): N/A</p> <p>If the Exporter is a Processor or Sub-Processor – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data:</p> <p>Name of agreement: N/A</p> <p>Date of agreement: N/A</p> <p>Parties to the agreement: N/A</p> <p>Reference (if any): N/A</p>
Term	<p>The Importer may Process the Transferred Data for the following time period:</p> <p><input type="checkbox"/> the period for which the Linked Agreement is in force</p> <p><input checked="" type="checkbox"/> time period:</p>

	<input type="checkbox"/> (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.
Ending the IDTA before the end of the Term	<input checked="" type="checkbox"/> the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing. <input type="checkbox"/> the Parties can end the IDTA before the end of the Term by serving: _____ months' written notice, as set out in Section 29 (How to end this IDTA without there being a breach).
Ending the IDTA when the Approved IDTA changes	Which Parties may end the IDTA as set out in Section 29.2: <input type="checkbox"/> Importer <input type="checkbox"/> Exporter <input checked="" type="checkbox"/> neither Party
Can the Importer make further transfers of the Transferred Data?	<input checked="" type="checkbox"/> The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data). <input type="checkbox"/> The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).
Specific restrictions when the Importer may transfer on the Transferred Data	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1: <input checked="" type="checkbox"/> if the Exporter tells it in writing that it may do so. <input type="checkbox"/> to: <input type="checkbox"/> to the authorised receivers (or the categories of authorised receivers) set out in: <input type="checkbox"/> there are no specific restrictions.
Review Dates	<input type="checkbox"/> No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data First review date: The Parties must review the Security Requirements at least once: <input type="checkbox"/> each _____ month(s) <input type="checkbox"/> each quarter <input type="checkbox"/> each 6 months

	<p>per each year</p> <p><input type="checkbox"/> each year(s)</p> <p><input type="checkbox"/> each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment</p>
--	--

Table 3: Transferred Data

Transferred Data	<p>The personal data to be sent to the Importer under this IDTA consists of:</p> <p><input checked="" type="checkbox"/> The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.</p>
Special Categories of Personal Data and criminal convictions and offences	<p>The Transferred Data includes data relating to:</p> <p><input type="checkbox"/> racial or ethnic origin</p> <p><input type="checkbox"/> political opinions</p> <p><input type="checkbox"/> religious or philosophical beliefs</p> <p><input type="checkbox"/> trade union membership</p> <p><input type="checkbox"/> genetic data</p> <p><input type="checkbox"/> biometric data for the purpose of uniquely identifying a natural person</p> <p><input type="checkbox"/> physical or mental health</p> <p><input type="checkbox"/> sex life or sexual orientation</p> <p><input type="checkbox"/> criminal convictions and offences</p> <p><input checked="" type="checkbox"/> none of the above</p> <p><input type="checkbox"/> set out in:</p> <p>And:</p> <p><input type="checkbox"/> The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to.</p>


	<p>þ The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.</p>
Relevant Data Subjects	<p>The Data Subjects of the Transferred Data are:</p> <p><input checked="" type="checkbox"/> The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.</p>
Purpose	<p><input type="checkbox"/> The Importer may Process the Transferred Data for the following purposes:</p> <p><input checked="" type="checkbox"/> The Importer may Process the Transferred Data for the purposes set out in:</p> <div data-bbox="564 936 616 994" data-label="Image"> </div> <p>20201028_Fournet Supplier Agreement_4</p> <p>In both cases, any other purposes which are compatible with the purposes set out above.</p> <p><input checked="" type="checkbox"/> The purposes will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.</p>

Table 4: Security Requirements


Security of Transmission	N/A
Security of Storage	As per security requirements set out in GDPR.
Security of Processing	N/A

Organisational security measures	N/A
Technical security minimum requirements	
Updates to the Security Requirements	<input checked="" type="checkbox"/> The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. <input type="checkbox"/> The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Part 2: Extra Protection Clauses

Extra Protection Clauses:	Those set out in Annex A of the linked agreement:  20201028_Fournet Supplier Agreement_4
(i) Extra technical security protections	N/A
(ii) Extra organisational protections	N/A
(iii) Extra contractual protections	N/A

Part 3: Commercial Clauses

Commercial Clauses	Those set out in Annex A:  20201028_Fournet Supplier Agreement_4
---------------------------	--

Information that helps you to understand this IDTA

1. This IDTA and Linked Agreements

- 1.1 Each Party agrees to be bound by the terms and conditions set out in the IDTA, in exchange for the other Party also agreeing to be bound by the IDTA.
- 1.2 This IDTA is made up of:
 - 1.2.1 Part one: Tables;
 - 1.2.2 Part two: Extra Protection Clauses;
 - 1.2.3 Part three: Commercial Clauses; and
 - 1.2.4 Part four: Mandatory Clauses.
- 1.3 The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.
- 1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties and which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).
- 1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.

2. Legal Meaning of Words

- 2.1 If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.
- 2.2 To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.

3. You have provided all the information required

- 3.1 The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.
- 3.2 In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:
 - 3.2.1 the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and
 - 3.2.2 the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.

- 3.3 In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.

4. How to sign the IDTA

- 4.1 The Parties may choose to each sign (or execute):
- 4.1.1 the same copy of this IDTA;
 - 4.1.2 two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;
 - 4.1.3 a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

5. Changing this IDTA

- 5.1 Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:
- 5.1.1 to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the cross-reference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;
 - 5.1.2 to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;
 - 5.1.3 so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or
 - 5.1.4 to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4;

provided that the changes do not reduce the Appropriate Safeguards.

- 5.2 If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 5.3 If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 5.4 From time to time, the ICO may publish a revised Approved IDTA which:
 - 5.4.1 makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or
 - 5.4.2 reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

6. Understanding this IDTA

- 6.1 This IDTA must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
- 6.2 If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.
- 6.3 If the meaning of the IDTA is unclear or there is more than one meaning, the meaning which most closely aligns with the UK Data Protection Laws applies.
- 6.4 Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party's liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.
- 6.5 If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.
- 6.6 The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.
- 6.7 If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):
 - 6.7.1 the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject's rights, in which case those terms will override the IDTA; and

- 6.7.2 a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.
- 6.8 The words “include”, “includes”, “including”, “in particular” are used to set out examples and not to set out a finite list.
- 6.9 References to:
 - 6.9.1 singular or plural words or people, also includes the plural or singular of those words or people;
 - 6.9.2 legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this IDTA has been signed; and
 - 6.9.3 any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

7. Which laws apply to this IDTA

- 7.1 This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

How this IDTA provides Appropriate Safeguards

8. The Appropriate Safeguards

- 8.1 The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:
 - 8.1.1 both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and
 - 8.1.2 the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.
- 8.2 The Exporter must:
 - 8.2.1 ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and
 - 8.2.2 (if the Importer reasonably requests) provide it with a copy of any TRA.
- 8.3 The Importer must:

- 8.3.1 before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the “Importer Information”);
 - 8.3.2 co-operate with the Exporter to ensure compliance with the Exporter’s obligations under the UK Data Protection Laws;
 - 8.3.3 review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and
 - 8.3.4 inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.
- 8.4 The Importer must ensure that at the Start Date and during the Term:
- 8.4.1 the Importer Information is accurate;
 - 8.4.2 it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.
- 8.5 Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.
- 9. Reviews to ensure the Appropriate Safeguards continue**
- 9.1 Each Party must:
- 9.1.1 review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and
 - 9.1.2 inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.
- 9.2 If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:
- 9.2.1 pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the

Appropriate Safeguards prior to the time the IDTA no longer provided
Appropriate Safeguards, but no other Processing;

9.2.2 agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and

9.2.3 where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.

10. The ICO

10.1 Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.

10.2 The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.

10.3 The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

The Exporter

11. Exporter's obligations

11.1 The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.

11.2 The Exporter must:

11.2.1 comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;

11.2.2 comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and

11.2.3 carry out reasonable checks on the Importer's ability to comply with this IDTA, and take appropriate action including under Section 9.2, Section 29 or Section 30, if at any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.

11.3 The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.

11.4 The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.

11.5 The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

The Importer

12. General Importer obligations

12.1 The Importer must:

- 12.1.1 only Process the Transferred Data for the Purpose;
- 12.1.2 comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;
- 12.1.3 comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;
- 12.1.4 keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;
- 12.1.5 if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and
- 12.1.6 if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).

12.2 The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.

13. Importer's obligations if it is subject to the UK Data Protection Laws

13.1 If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:

- 13.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and
- 13.1.2 it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.

13.2 If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:

- Section 14 (Importer's obligations to comply with key data protection principles);
- Section 15 (What happens if there is an Importer Personal Data Breach);
- Section 15 (How Relevant Data Subjects can exercise their data subject rights); and
- Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor).

14. Importer's obligations to comply with key data protection principles

- 14.1 The Importer does not need to comply with this Section 14 if it is the Exporter's Processor or Sub-Processor.
- 14.2 The Importer must:
 - 14.2.1 ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;
 - 14.2.2 ensure that the Transferred Data it Processes is accurate and (where necessary) kept up to date, and (where appropriate considering the Purposes) correct or delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and
 - 14.2.3 ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.
- 15. What happens if there is an Importer Personal Data Breach**
- 15.1 If there is an Importer Personal Data Breach, the Importer must:
 - 15.1.1 take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter's Processor or Sub-Processor: these steps must comply with the Exporter's instructions and the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller; and
 - 15.1.2 ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.
- 15.2 If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:
 - 15.2.1 notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:
 - 15.2.1.1 a description of the nature of the Importer Personal Data Breach;
 - 15.2.1.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
 - 15.2.1.3 likely consequences of the Importer Personal Data Breach;
 - 15.2.1.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;
 - 15.2.1.5 contact point for more information; and
 - 15.2.1.6 any other information reasonably requested by the Exporter,

- 15.2.2 if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and
 - 15.2.3 assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.
- 15.3 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:
- 15.3.1 a description of the nature of the Importer Personal Data Breach;
 - 15.3.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
 - 15.3.3 likely consequences of the Importer Personal Data Breach;
 - 15.3.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;
 - 15.3.5 contact point for more information; and
 - 15.3.6 any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.

- 15.4 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform those Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.
- 15.5 The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

16. Transferring on the Transferred Data

- 16.1 The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:

- 16.1.1 the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or
- 16.1.2 the third party has been added to this IDTA as a Party; or
- 16.1.3 if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or
- 16.1.4 if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or
- 16.1.5 the transfer is to the UK or an Adequate Country.
- 16.2 The Importer does not need to comply with Section 16.1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).
- 17. Importer's responsibility if it authorises others to perform its obligations**
- 17.1 The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).
- 17.2 If the Importer is the Exporter's Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.
- 17.3 The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.
- 17.4 The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has sub-contracted any obligations to its Processors and Sub-Processors, or authorised an employee or other person to perform them (and references to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).

What rights do individuals have?

18. The right to a copy of the IDTA

- 18.1 If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:
 - 18.1.1 it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;
 - 18.1.2 it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;
 - 18.1.3 it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Data Subject with a

summary of those redactions so that the Relevant Data Subject can understand the content of the Tables or the information provided from the Linked Agreement.

19. The right to Information about the Importer and its Processing

19.1 The Importer does not need to comply with this Section 19 if it is the Exporter's Processor or Sub-Processor.

19.2 The Importer must ensure that each Relevant Data Subject is provided with details of:

the Importer (including contact details and the Importer Data Subject Contact);

- the Purposes; and
- any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

19.3 The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.

19.4 The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

20. How Relevant Data Subjects can exercise their data subject rights

20.1 The Importer does not need to comply with this Section 20 if it is the Exporter's Processor or Sub-Processor.

20.2 If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.

20.3 The following Sections of this Section 20, relate to a Relevant Data Subject's Personal Data which forms part of the Transferred Data the Importer is Processing.

20.4 If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:

- 20.4.1 Without Undue Delay (and in any event within one month);
- 20.4.2 at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;
- 20.4.3 in clear and plain English that is easy to understand; and
- 20.4.4 in an easily accessible form

together with

- 20.4.5 (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and
- 20.4.6 information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.
- 20.5 If a Relevant Data Subject requests, the Importer must:
 - 20.5.1 rectify inaccurate or incomplete Transferred Data;
 - 20.5.2 erase Transferred Data if it is being Processed in breach of this IDTA;
 - 20.5.3 cease using it for direct marketing purposes; and
 - 20.5.4 comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.
- 20.6 The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated processing, including profiling (the “Decision-Making”), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:
 - 20.6.1 the Relevant Data Subject has given their explicit consent to such Decision-Making; or
 - 20.6.2 Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK; or
 - 20.6.3 the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.
- 21. How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter’s Processor or Sub-Processor**
- 21.1 Where the Importer is the Exporter’s Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.
- 22. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws**
- 22.1 The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:
 - 22.1.1 it is unable to reasonably verify the identity of an individual making the request; or

22.1.2 the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee; or

22.1.3 a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual's request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.

How to give third parties access to Transferred Data under Local Laws

23. Access requests and direct access

23.1 In this Section 23 an "Access Request" is a legally binding request (except for requests only binding by contract law) to access any Transferred Data and "Direct Access" means direct access to any Transferred Data by public authorities of which the Importer is aware.

23.2 The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.

23.3 In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.

23.4 In so far as Local Laws allow, the Importer must:

23.4.1 make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and

23.4.2 provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.

24. Giving notice

24.1 If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.

24.2 If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving Party's next normal business day, and provided no notice of non-delivery or bounceback is received.

24.3 The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.

25. General clauses

- 25.1 In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:
- 25.1.1 contain all the terms and conditions agreed by the Parties; and
 - 25.1.2 override all previous contacts and arrangements, whether oral or in writing.
- 25.2 If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.
- 25.3 Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.
- 25.4 Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.
- 25.5 This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.
- 25.6 If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.
- 25.7 If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.
- 25.8 If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:
- 25.8.1 it only applies in so far as it explicitly waives specific rights or remedies;
 - 25.8.2 it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and
 - 25.8.3 it will not prevent that Party from enforcing any other right or remedy in future.

What happens if there is a breach of this IDTA?

26. Breaches of this IDTA

- 26.1 Each Party must notify the other Party in writing (and with all relevant details) if it:
- 26.1.1 has breached this IDTA; or
 - 26.1.2 it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.

26.2 In this IDTA “Significant Harmful Impact” means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.

27. Breaches of this IDTA by the Importer

27.1 If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.

27.2 Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:

27.2.1 the Exporter must suspend sending Transferred Data to the Importer;

27.2.2 If the Importer is the Exporter’s Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and

27.2.3 if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:

27.2.3.1 notify the third party receiver of the breach and suspend sending it Transferred Data; and

27.2.3.2 if the third party receiver is the Importer’s Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).

27.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 30.1.

28. Breaches of this IDTA by the Exporter

28.1 If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.

28.2 Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.

28.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 30.1.

Ending the IDTA

29. How to end this IDTA without there being a breach

- 29.1 The IDTA will end:
 - 29.1.1 at the end of the Term stated in Table 2: Transfer Details; or
 - 29.1.2 if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;
 - 29.1.3 at any time that the Parties agree in writing that it will end; or
 - 29.1.4 at the time set out in Section 29.2.
- 29.2 If the ICO issues a revised Approved IDTA under Section 5.4, if any Party selected in Table 2 “Ending the IDTA when the Approved IDTA changes”, will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:
 - 29.2.1 its direct costs of performing its obligations under the IDTA; and/or
 - 29.2.2 its risk under the IDTA,

and in either case it has first taken reasonable steps to reduce that cost or risk so that it is not substantial and disproportionate, that Party may end the IDTA at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved IDTA.

30. How to end this IDTA if there is a breach

- 30.1 A Party may end this IDTA immediately by giving the other Party written notice if:
 - 30.1.1 the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and
 - 30.1.1.1 the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or
 - 30.1.1.2 the breach and its Significant Harmful Impact cannot be corrected;
 - 30.1.2 the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

31. What must the Parties do when the IDTA ends?

- 31.1 If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:
 - 31.1.1 notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;

- 31.1.2 retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and
- 31.1.3 stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 29 will apply.
- 31.2 When this IDTA ends (no matter what the reason is):
 - 31.2.1 the Exporter must stop sending Transferred Data to the Importer; and
 - 31.2.2 if the Importer is the Exporter's Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;
 - 31.2.3 if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.
 - 31.2.4 the following provisions will continue in force after this IDTA ends (no matter what the reason is):

Section 1 (This IDTA and Linked Agreements);

Section 2 (Legal Meaning of Words);

Section 6 (Understanding this IDTA);

Section 7 (Which laws apply to this IDTA);

Section 10 (The ICO);

Sections 11.1 and 11.4 (Exporter's obligations);

Sections 12.1.2, 12.1.3, 12.1.4, 12.1.5 and 12.1.6 (General Importer obligations);

Section 13.1 (Importer's obligations if it is subject to UK Data Protection Laws);

Section 17 (Importer's responsibility if it authorised others to perform its obligations);

Section 24 (Giving notice);

Section 25 (General clauses);

Section 31 (What must the Parties do when the IDTA ends);

Section 32 (Your liability);

Section 33 (How Relevant Data Subjects and the ICO may bring legal claims);

Section 34 (Courts legal claims can be brought in);

Section 35 (Arbitration); and

Section 36 (Legal Glossary).

How to bring a legal claim under this IDTA

32. Your liability

- 32.1 The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.
- 32.2 Each Party (in this Section, “Party One”) agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:
- 32.2.1 Party One’s breach of this IDTA; and/or
 - 32.2.2 where Party One is a Processor, Party One’s breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;
 - 32.2.3 where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One’s Processing of the Transferred Data (no matter how minimal)

in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.

- 32.3 If one Party has paid compensation to a Relevant Data Subject under Section 32.2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party’s responsibility for the damage, so that the compensation is fairly divided between the Parties.
- 32.4 The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

33. How Relevant Data Subjects and the ICO may bring legal claims

- 33.1 The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):
- **Section 1** (This IDTA and Linked Agreements);
 - **Section 3** (You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses);
 - **Section 8** (The Appropriate Safeguards);
 - **Section 9** (Reviews to ensure the Appropriate Safeguards continue);
 - **Section 11** (Exporter’s obligations);
 - **Section 12** (General Importer Obligations);
 - **Section 13** (Importer’s obligations if it is subject to UK Data Protection Laws);
 - **Section 14** (Importer’s obligations to comply with key data protection laws);
 - **Section 15** (What happens if there is an Importer Personal Data Breach);
 - **Section 16** (Transferring on the Transferred Data);

- **Section 17** (Importer's responsibility if it authorises others to perform its obligations);
 - **Section 18** (The right to a copy of the IDTA);
 - **Section 19** (The Importer's contact details for the Relevant Data Subjects);
 - **Section 20** (How Relevant Data Subjects can exercise their data subject rights);
 - **Section 21** (How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor);
 - **Section 23** (Access Requests and Direct Access);
 - **Section 26** (Breaches of this IDTA);
 - **Section 27** (Breaches of this IDTA by the Importer);
 - **Section 28** (Breaches of this IDTA by the Exporter);
 - **Section 30** (How to end this IDTA if there is a breach);
 - **Section 31** (What must the Parties do when the IDTA ends); and
 - any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.
- 33.2 The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10 (The ICO), Sections 11.1 and 11.2 (Exporter's obligations), Section 12.1.6 (General Importer obligations) and Section 13 (Importer's obligations if it is subject to UK Data Protection Laws).
- 33.3 No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).
- 33.4 The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.
- 33.5 In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.
- 34. Courts legal claims can be brought in**
- 34.1 The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).
- 34.2 The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.
- 34.3 The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details
- 34.4 Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.5 Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).

35. Arbitration

35.1 Instead of bringing a claim in a court under Section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section 35.

35.2 The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section 35.

35.3 There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.

35.4 London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the 'primary place for legal claims to be made' in Table 2: Transfer Details.

35.5 The English language must be used in the arbitral proceedings.

35.6 English law governs this Section 35. This applies regardless of whether or not the parties selected a different UK country's law as the 'UK country's law that governs the IDTA' in Table 2: Transfer Details.

36. Legal Glossary

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Access Request	As defined in Section 23, as a legally binding request (except for requests only binding by contract law) to access any Transferred Data.
Adequate Country	A third country, or: a territory; one or more sectors or organisations within a third country; an international organisation; which the Secretary of State has specified by regulations provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018.
Appropriate Safeguards	The standard of protection over the Transferred Data and of the Relevant Data Subject's rights, which is required by UK Data Protection Laws when

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
	you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved IDTA	The template IDTA A1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4.
Commercial Clauses	The commercial clauses set out in Part three.
Controller	As defined in the UK GDPR.
Damage	All material and non-material loss and damage.
Data Subject	As defined in the UK GDPR.
Decision-Making	As defined in Section 20.6, as decisions about the Relevant Data Subjects based solely on automated processing, including profiling, using the Transferred Data.
Direct Access	As defined in Section 23 as direct access to any Transferred Data by public authorities of which the Importer is aware.
Exporter	The exporter identified in Table 1: Parties & Signature.
Extra Protection Clauses	The clauses set out in Part two: Extra Protection Clauses.
ICO	The Information Commissioner.
Importer	The importer identified in Table 1: Parties & Signature.
Importer Data Subject Contact	The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19.
Importer Information	As defined in Section 8.3.1, as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including for the Exporter to carry out any TRA.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Importer Personal Data Breach	A 'personal data breach' as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer.
Linked Agreement	The linked agreements set out in Table 2: Transfer Details (if any).
Local Laws	Laws which are not the laws of the UK and which bind the Importer.
Mandatory Clauses	Part four: Mandatory Clauses of this IDTA.
Notice Period	As set out in Table 2: Transfer Details.
Party/Parties	The parties to this IDTA as set out in Table 1: Parties & Signature.
Personal Data	As defined in the UK GDPR.
Personal Data Breach	As defined in the UK GDPR.
Processing	As defined in the UK GDPR. When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer's behalf.
Processor	As defined in the UK GDPR.
Purpose	The 'Purpose' set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to.
Relevant Data Subject	A Data Subject of the Transferred Data.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR
Review Dates	The review dates or period for the Security Requirements set out in Table 2: Transfer Details, and any review dates set out in any revised Approved IDTA.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Significant Harmful Impact	As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Data Subject or the other Party.
Special Category Data	As described in the UK GDPR, together with criminal conviction or criminal offence data.
Start Date	As set out in Table 1: Parties and signature.
Sub-Processor	A Processor appointed by another Processor to Process Personal Data on its behalf. This includes Sub-Processors of any level, for example a Sub-Sub-Processor.
Tables	The Tables set out in Part one of this IDTA.
Term	As set out in Table 2: Transfer Details.
Third Party Controller	The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor If there is not a Third Party Controller this can be disregarded.
Transfer Risk Assessment or TRA	A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards
Transferred Data	Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in Section 3 of the Data Protection Act 2018.
Without Undue Delay	Without undue delay, as that phrase is interpreted in the UK GDPR.

Alternative Part 4 Mandatory Clauses:

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.
--------------------------	--

ANNEX 2 TO STANDARD CONTRACTUAL CLAUSES
EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE
DIRECTORATE C: FUNDAMENTAL RIGHTS AND UNION CITIZENSHIP UNIT
C.3: DATA PROTECTION
COMMISSION DECISION C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation:

Address:

.....

(the data exporter)

And

Name of the data importing organisation:

Address:

.....

(the data importer)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);
- (b) 'the data exporter' means the controller who transfers the personal data;
- (c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data

exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

- (g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer (2)

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
 - (ii) any accidental or unauthorised access; and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data

exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

- 1.The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a)to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b)to refer the dispute to the courts in the Member State in which the data exporter is established.
- 2.The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

- 1.The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
- 2.The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
- 3.The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely ...

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (3). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely ...
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2.The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): ...

Position: ...

Address: ...

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): ...

Position: ...

Address: ...

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

...

...

...

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

APAC Remote Support Limited

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Customer Names, Phone Numbers and Email Addresses.

Categories of data

The personal data transferred concern the following categories of data (please specify):

No Personal Data other than that listed above is held.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

No Special categories of data is held.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

To enable engineers to assist with fault resolution. The data is stored securely in a GDPR Compliant cloud solution.

DATA EXPORTER

Name:

Authorised Signature

DATA IMPORTER

Name:

Authorised Signature

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

General GDPR training provided to staff. Data is not stored locally; it is stored in a cloud based GDPR compliant solution and user access entitlement reviews are conducted annually or as required when staff join or leave APAC remote support.

DATA EXPORTER

Name:

Authorised Signature

DATA IMPORTER

Name:

Authorised Signature

