BASIC PURCHASE TERMS AND CONDITIONS

Contents

1. Definitions and Interpretation

1.1 In this Contract the following definitions apply:

"Bribery Laws" means the Bribery Act 2010 and all other applicable UK legislation, statutory instruments and regulations in relation to bribery or corruption and any similar or equivalent legislation in any other relevant jurisdiction;

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

"Confidential Information" means any information of a confidential nature concerning the business, assets, affairs, customers, clients or suppliers of the other party or of any member of its company, including information relating to a party's operations, processes, plans, product information, know-how, designs, trade secrets, software, market opportunities and customers, or which is developed by or on behalf of Wightlink in performing its obligations under, or otherwise pursuant to the Contract;

"Contract" means the agreement between the Supplier and Wightlink for the sale and purchase of the Deliverables following an accepted Purchase Order, in accordance with these terms and conditions ("Conditions");

"Data Protection Laws" means all applicable data protection and privacy laws that apply in the UK from time to time including the Data Protection Act 2018, and the UK GDPR and any associated national implementing laws, regulations and secondary legislation.

"Deliverables" means all articles, materials, goods, work or services specified in the Purchase Order or as may be amended from time to time;

"Force Majeure" means an event or sequence of events beyond any party's reasonable control (after exercise of reasonable care to put in place robust back-up and disaster recovery arrangements) preventing or delaying it from performing its obligations under the Contract including an act of god, fire, flood, lightning, earthquake or other natural disaster; war, riot or civil unrest; strike, lockout or boycott or other industrial action except strikes or other industrial disputes involving the Supplier's or its suppliers' workforce or subcontractors;

"UK GDPR" means the United Kingdom General Data Protection Regulation, as it forms part of the law of the UK by virtue of section 3 of the European Union (Withdrawal) Act 2018";

"Intellectual Property Rights" means copyright, patents, know-how, trade secrets, trademarks, trade names, design rights, rights in get-up, rights in goodwill, rights in confidential information, rights to sue for passing off, domain names and all similar rights and, in each case:

(a) whether registered or not

(b) including any applications to protect or register such rights

(c) including all renewals and extensions of such rights or applications

(d) whether vested, contingent or future

(e) to which the relevant party is or may be entitled, and

(f) in whichever part of the world existing;

"Location" means the address(es) for delivery of the Deliverables as set out in the Purchase Order;

"Process/Processing/Processed", "Controller", "Processor", "Data Subject", "Personal Data", "Special Categories of Personal Data" shall have the same meaning as in Data Protection Laws;

"Purchase Order" means document through which Wightlink may place an order for Deliverables from the Supplier which shall include (among other things) the number of subscriptions, goods and other services contracted for, the applicable fees, the billing period, and any other charges as agreed by the parties from time to time;

"Specification" means the description or specification of the Deliverables set out or referred to in the Purchase Order including any related plans and drawings as agreed in writing by Wightlink;

"Supplier" means the person who sells the Deliverables to Wightlink and whose details are set out in the Purchase Order; and

"Wightlink" means Wightlink Limited, a company incorporated in England and Wales (company no. 01059267) whose registered address is at Gunwharf Terminal, Gunwharf Road, Portsmouth, Hampshire, PO1 2LA.

1.2 In this Contract the following interpretation apply:

(a) References to person includes a natural person, corporate or unincorporated body (whether or not having separate legal personality).

(b) References to a party includes its successors and permitted assigns.

(c) References to legislation or a legislative provision is to it as amended or re-enacted. A reference to legislation or a legislative provision includes all subordinate legislation made under that legislation or legislative provision.

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

(e) A reference to writing or written includes email.

2. Application of these Conditions

2.1 These Conditions and any Purchase Order agreed by the parties apply to and form part of the Contract between the Supplier and Wightlink.

2.2 No terms or conditions endorsed on, delivered with, or contained in the Supplier's quotation, sales conditions, confirmation of order, specification or other document shall form part of this Contract except to the extent that Wightlink otherwise agrees in writing.

2.3 No variation of this Contract shall be binding unless expressly agreed in writing and executed by a duly authorised signatory on behalf of Wightlink.

2.4 Each Purchase Order from Wightlink to the Supplier shall be an offer to purchase Deliverables subject to these Conditions.

2.5 No Purchase Order shall bind the Supplier unless and until it bears a Purchase Order number.

2.6 A Purchase Order may be withdrawn or amended by Wightlink at any time before acceptance by the Supplier. If the Supplier is unable to accept a Purchase Order, it shall notify Wightlink promptly in writing no later than 7 days of receipt of the Purchase Order.

2.7 Acceptance of a Purchase Order by the Supplier shall take place by written acceptance of the same, or by any other conduct of the Supplier which Wightlink reasonably considers is consistent with acceptance of Purchase Orders or where the Supplier has not responded within 7 days of receipt of the Order.

2.8 The Supplier shall be under no responsibility to accept a Purchase Order for any Deliverables which has not been properly submitted by Wightlink where Wightlink has been notified of this error and it has failed to rectify this within 7 days. Deliveries of any Deliverables other than those in accordance with a Purchase Order may (at Wightlink's option) be returned to the Supplier at the Supplier's expense and risk.

3. Price

3.1 The price for the Deliverables shall be as set out in the Purchase Order (or any special conditions agreed with Wightlink) and shall be exclusive of any applicable value added tax ("VAT"). VAT shall be charged by the Supplier at the then applicable rate and payable by Wightlink only on receipt of a valid VAT invoice).

3.2 No increase in the price may be made after the Purchase Order is placed, unless agreed with Wightlink.

3.3 The price shall be the full and exclusive remuneration of the Supplier in respect of the performance of the Deliverables.

3.4 Unless otherwise agreed in writing by Wightlink, the charges shall include every cost and expense of the Supplier directly or indirectly incurred in connection with the performance of the Deliverables.

3.5 The price includes all packaging, delivery and unloading required. No extra charges shall be effective unless agreed in writing and signed by Wightlink.

4. Payment

4.1 The Supplier shall invoice Wightlink at the address detailed on the front of the Purchase Order after delivery (or before if otherwise agreed). It shall contain the Purchase Order.

4.2 The Supplier shall invoice Wightlink for the Deliverables no sooner than completion of delivery of the Deliverables as set out in clause 6 or, if later, Wightlinks' acceptance of the Deliverables.

4.3 Where sums due under the Contract are not paid in full by the due date, the defaulting party shall pay interest on the overdue sum from the due date until payment of the overdue sum, whether before or after judgment at the rate of two per cent per annum above the Bank of England's base rate. All parties acknowledge that this is a substantial remedy for the purposes of the Late Payment of Commercial Debts (Interest) Act 1998.

4.4 Wightlink shall, except in where payment is disputed and subject to receipt of the necessary invoice, pay for the Deliverables within 30 days of the date of receiving the invoice or by such other time as may be agreed between the parties.

4.5 All invoices raised by the Supplier must display the Supplier's name, company registration number, date of the Purchase Order, Purchase Order number, the invoice number and, where applicable, the VAT number and any VAT due on the invoice or in a format as otherwise stated by Wightlink. The Supplier must also include all supporting documentation applicable to the invoice including, but not limited to, valid receipts for expenses, signed timesheets and vessel stamp. Wightlink shall not be liable for any payment delay resulting from the Supplier's failure to comply with this clause.

5. Cancellation

5.1 Wightlink shall have the right to cancel the Purchase Order for the Deliverables or for any part of the Deliverables which have not yet been performed for Wightlink.

6. Delivery and Performance

6.1 Deliverables shall be delivered by the Supplier to the Location on the date(s) and times specified in the Purchase Order or as otherwise agreed between the parties.

6.2 Deliverables shall be deemed delivered by the Supplier only on receipt of the Deliverables by an authorised representative of Wightlink at the Location.

6.3 If the Deliverables are to be delivered in installments the Contract must, unless otherwise agreed by Wightlink in writing, be treated as a single Contract and not severable.

6.4 The Supplier shall ensure that the Deliverables shall:

6.4.1 correspond with their description and any applicable Specification;

6.4.2 be properly packed and secured in such manner as to enable them to reach the Location in good condition;

6.4.3 be of satisfactory quality (within the meaning of the Sale of Goods Act 1979) and fit for any purpose held out by the Supplier or made known to the Supplier by Wightlink, expressly or by implication, and in this respect Wightlink relies on the Supplier's skill and judgement;

6.4.4 where they are manufactured products, be free from defects in design, materials and workmanship and remain so for 12 months after delivery; and

6.4.5 comply with all applicable statutory and regulatory requirements relating to the manufacture, labelling, packaging, storage, handling and delivery of the deliverables.

6.4.6 obtain and at all times maintain all licences and consents which may be required for the provision of the Deliverables;

6.4.7 observe all health and safety rules and regulations and any other security requirements that apply at any of Wightlink's premises;

6.4.8 hold all materials, equipment and tools, drawings, specifications and data supplied by Wightlink to the Supplier in safe custody at its own risk, maintain materials in good condition until returned to Wightlink, and not dispose or use materials other than in accordance with Wightlink's written instructions or authorisation; and

6.4.9 not do or omit to do anything which may cause Wightlink to lose any licence, authority, consent or permission upon which it relies for the purposes of conducting its business, and the Supplier acknowledges that Wightlink may rely or act on the Deliverables.

6.5 If the Supplier requires Wightlink to return any packaging material to the Supplier, this must be clearly stated on the delivery note. Any such packaging material shall be returned to the Supplier at the cost of the Supplier.

6.6 The Deliverables shall not be delivered by or performed in instalments unless otherwise agreed in writing by Wightlink and specified in special conditions below.

6.7 Time of delivery or performance (as the case may be) is of the essence. If the Supplier fails to deliver any of the Deliverables by the date specified in the Purchase Order, Wightlink shall (without prejudice to its other rights and remedies) be entitled at Wightlink's sole discretion:

6.7.1 to terminate the Contract in whole or in part;

6.7.2 to refuse to accept any subsequent performance of the Deliverables which the Supplier attempts to make;

6.7.3 to purchase the same or similar Deliverables from a supplier other than the Supplier;

6.7.4 to recover from the Supplier all costs and losses resulting to Wightlink, including the amount by which the price payable by Wightlink to acquire those Deliverables from another supplier exceeds the price payable under the Contract and any loss of profit;

6.7.5 to require a refund from the Supplier of sums paid in advance for Deliverables that the Supplier has not provided and/or delivered;

6.7.6 to claim damages for any additional costs, loss or expenses incurred by Wightlink which are in any way attributable to the Supplier's failure to meet such dates and timescales; and

6.7.7 all or any of the foregoing.

7. Acceptance, Rejection and Inspection

7.1 Wightlink shall not have accepted, or be deemed to have accepted, the Deliverables until the conditions as defined in clause 7.2, are fulfilled ("Acceptance Conditions").

7.2 The Acceptance Conditions are that:

7.2.1 Deliverables have been performed at the Location; and

7.2.2 Wightlink has notified the Supplier in writing that the Deliverables have been delivered or performed (as the case may be) in full compliance with the Contract.

7.3 Wightlink shall be entitled to reject any Deliverables which are not in full compliance with the Conditions of the Contract. Any acceptance of defective, late or incomplete Deliverables or any payment made in respect thereof, shall not constitute a waiver of any of Wightlink's rights and remedies, including its right to reject. If the Deliverables are rejected due to the volume of the Deliverables exceeding the tolerances (if any) specified in the Purchase Order, the Supplier shall promptly and at its own cost arrange for redelivery of the correct volume.

7.4 Any rejected Deliverables may be returned to the Supplier by Wightlink at the Supplier's cost and risk. The Supplier shall pay to Wightlink a reasonable charge for storing and returning any of the Deliverables over-delivered or rejected.

7.5 The Supplier shall always ensure that it has and maintains all the licences, permissions, authorisations, consents and permits that it needs to carry out its obligations under the Contract in respect of the Deliverables.

8. Title and Risk

8.1 All property and title in the Deliverables shall pass to Wightlink (without prejudice to any right of rejection) upon payment for the Deliverables being made to the Supplier.

8.2 Risk of the Deliverables shall pass to Wightlink upon proper delivery of the Deliverables.

9. Warranty

9.1 The Supplier warrants and represents that, for a period of 12 months from Wightlink's acceptance (the Warranty Period), the Deliverables shall:

9.1.1 conform to any sample, their description and to the Specification;

9.1.2 be free from defects in design, material and workmanship;

9.1.3 comply with all applicable laws, standards and best industry practice;

9.1.4 if Deliverables, be of satisfactory quality within the meaning of the Sale of Goods Act 1979;

9.1.5 if Deliverables, be supplied with reasonable care and skill within the meaning of the Supply of Goods and Services Act 1982, Part II, s 13; and

9.1.6 be fit for purpose and any purpose held out by the Supplier and set out in the Purchase Order.

9.2 Wightlink may reject any Deliverables that does not comply with clause 9.1 and the Supplier shall, at Wightlink's option, promptly remedy, repair, replace, correct, re-perform or refund the price of any such Deliverables provided that Wightlink serves a written notice on the Supplier within the warranty period that some or all of the Deliverables do not comply with clause 9.1.

9.3 The provisions of this Contract shall apply to any Deliverables that are remedied, repaired, replaced, corrected or re-performed with effect from the date of the delivery or performance of the remedied, repaired, replaced, corrected or re-performed Deliverables.

9.4 The Supplier also warrants that it shall comply with Wightlink's Code of Conduct (Schedule 1) as amended from time to time.

10. Anti-Bribery

10.1 Each party shall comply with the Bribery Act 2010 including ensuring that it has in place adequate procedures to prevent bribery and use all reasonable endeavours to ensure that:

10.1.1 all of that party's personnel;

10.1.2 all others associated with that party; and

10.1.3 all of that party's subcontractors involved in performing the Contract so comply.

11. Indemnity

11.1 The Supplier shall indemnify and keep indemnified, Wightlink from and against all losses, damages, liability, costs (including legal fees) and expenses incurred by Wightlink as a result of:

11.1.1 defective workmanship, quality or material breach;

11.1.2 any claim made against Wightlink in respect of any loss sustained by the Supplier's employees or third party to the extent that such loss was caused by, relates to or arises from the Deliverables;

11.1.3 any liability under the Consumer Protection Act 1987 in respect of the Deliverables; and

11.1.4 any act or omission of the Supplier, its employees or subcontractors in supplying, delivering and installing the Deliverables and the performance of any Deliverables, save in so far as such losses arise directly from the Suppliers negligence.

11.2 The Supplier shall indemnify and keep indemnified Wightlink from breach of any of the Supplier's obligations under this Contract (including any direct, penalties and legal costs (calculated on a full indemnity basis) and all other professional costs and expenses) suffered or incurred by Wightlink arising out of or in connection with:

11.2.1 any claim made against Wightlink for actual or alleged infringement of a third party's intellectual property rights arising out of, or in connection with, the manufacture, supply or use of the Deliverables;

11.2.2 any claim made against Wightlink arising out of or in connection with the Supplier's breach of clause 16 of this Contract (Processing of Personal Data) and any of its obligations under Data Protection Laws; and

11.2.3 any claim made against Wightlink by a third party arising out of or in connection with the supply of the Deliverables.

12. Insurance

12.1 During the term of this Contract and for a period of six years thereafter, the Supplier shall maintain in force, with a reputable insurance company, professional indemnity insurance, product liability insurance and public liability insurance to cover the liabilities that may arise under or in connection with this Contract, and shall, on Wightlink's request, produce both the insurance certificate giving details of cover and the receipt for the current year's premium in respect of each insurance.

13. Limitation of Liability

13.1 Notwithstanding any other provision of this Contract, the liability of the parties shall not be limited in any way in respect of the following:

13.1.1 death or personal injury caused by negligence;

13.1.2 fraud or fraudulent misrepresentation;

13.1.3 any other losses which cannot be excluded or limited by applicable law;

13.1.4 any losses caused by wilful misconduct.

13.2 Subject to clauses 13.1, Wightlink's total liability under this Contract shall not exceed the amount paid in relation to each relevant Purchase Order.

13.3 Subject to clause 13.1, neither Wightlink and the Supplier shall in any circumstances be liable, under or in connection with this Contract, for any consequential or indirect loss or damage of any kind.

14. Intellectual Property Rights

14.1 All specifications provided by Wightlink and all Intellectual Property Rights in the Deliverables made or performed in accordance with such specifications shall vest in and remain at all times the property of Wightlink and such specifications may only be used by the Supplier as necessary to perform the Contract. The Supplier assigns (or shall procure the assignment) to Wightlink absolutely, with full title guarantee, all right, title and interest in any such Intellectual Property Rights, and the Supplier shall do all such things and sign all documents necessary in Wightlink's opinion to vest all such Intellectual Property Rights in Wightlink, and to enable Wightlink to defend and enforce such Intellectual Property Rights, and the Supplier shall at Wightlink's request waive or procure a waiver of any applicable moral rights.

14.2 The Supplier shall indemnify Wightlink from and against any losses, damages, liability, costs (including legal fees) and expenses incurred by Wightlink as a result of or in connection with any action, demand or claim that use or possession of any of the Intellectual Property Rights, infringes the Intellectual Property Rights of any third party (a Supplier IPR Claim).

15. Confidentiality

15.1 The Supplier shall keep confidential all Confidential Information of Wightlink and shall only use the same as required to perform the Contract. The provisions of this clause shall not apply to:

15.1.1 any information which was in the public domain at the date of the Contract;

15.1.2 any information which comes into the public domain subsequently other than as a consequence of any breach of the Contract or any related agreement;

15.1.3 any information which is independently developed by the Supplier without using information supplied by Wightlink; or

15.1.4 any disclosure required by law or a regulatory authority or otherwise by the provisions of the Contract.

15.2 This clause shall remain in force in perpetuity.

16. Processing of Personal Data

16.1 Each party warrants that it shall at all times fully comply with its obligations under all relevant Data Protection Laws and shall not perform their obligations under the Contract in such a way as to cause the other party to breach any of its applicable obligations under the Data Protection Laws.

16.2 The Supplier shall fully indemnify and keep indemnified Wightlink against:

16.2.1 all losses, claims, damages, liabilities, fines, interest, penalties, costs, charges, sanctions, expenses, compensation paid to Data Subjects (including compensation to protect goodwill and ex gratia payments),

demands and legal and other professional costs (calculated on a full indemnity basis and in each case whether or not arising from any investigation by, or imposed by, a supervisory authority) arising out of or in connection with any breach by the Supplier of its obligations under this clause 16; and

16.2.2 all amounts paid or payable by Wightlink to a third party which would not have been paid or payable if the Supplier's breach of this clause 16 had not occurred.

16.3 Should the Supplier be deemed a Processor then the parties will enter into a separate Data Processing Agreement as set detailed in Schedule 2.

17. Force Majeure

17.1 A party shall not be liable if delayed in or prevented from performing its obligations due to Force Majeure, provided that it:

17.1.1 promptly notifies the other of the Force Majeure event and its expected duration; and

17.1.2 uses best endeavors to minimise the effects of that event.

17.2 If, due to Force Majeure, a party:

17.2.1 is or shall be unable to perform a material obligation; or

17.2.2 is delayed in or prevented from performing its obligations for a continuous period exceeding 14 days or total of more than 30 days in any consecutive period of 60 days; the other party may terminate the Contract on immediate notice.

18. Termination

18.1 Wightlink may terminate the Contract or any other contract which it has with the Supplier at any time by giving notice in writing to the Supplier if:

18.1.1 the Supplier commits a material breach of the Contract and such breach is not remediable;

18.1.2 the Supplier commits a material breach of the Contract which is not remedied within 14 days of receiving written notice of such breach; or

18.1.3 any consent, licence or authorisation held by the Supplier is revoked or modified such that the Supplier is no longer able to comply with its obligations under the Contract or receive any benefit to which it is entitled.

18.2 Wightlink may terminate the Contract at any time by giving notice in writing to the Supplier if the Supplier:

18.2.1 stops carrying on all or a significant part of its business, or indicates in any way that it intends to do so;

18.2.2 is unable to pay its debts either within the meaning of section 123 of the Insolvency Act 1986 or if Wightlink reasonably believes that to be the case;

18.2.3 becomes the subject of a company voluntary arrangement under the Insolvency Act 1986;

18.2.4 has a receiver, manager, administrator or administrative receiver appointed over all or any part of its undertaking, assets or income;

18.2.5 has a resolution passed for its winding up;

18.2.6 has a petition presented to any court for its winding up or an application is made for an administration order, or any winding-up or administration order is made against it;

18.2.7 is subject to any procedure for the taking control of its goods that is not withdrawn or discharged within 7 days of that procedure being commenced;

18.2.8 has a freezing order made against it;

18.2.9 is subject to any recovery or attempted recovery of items supplied to it by a supplier retaining title in those items;

18.2.10 is subject to any events or circumstances analogous to those in clauses 18.2.1 to 18.2.9 in any jurisdiction;

18.3 Termination or expiry of the Contract shall not affect any accrued rights and liabilities of Wightlink at any time up to the date of termination.

19. Notices

19.1 Any notice given to a party under or in connection with the Contract shall be in writing and shall be:

19.1.1 delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or

19.1.2 sent by email to the following addresses (or an address substituted in writing by the party to be served):

19.2 Any notice shall be deemed to have been received:

19.2.1 if delivered by hand, at the time the notice is left at the proper address;

19.2.2 if sent by pre-paid first-class post or other next working day delivery service, at 9.00 am on the second Business Day after posting; or

19.2.3 if sent by email, at the time of transmission, or, if this time falls outside the relevant party's business hours in the place of receipt, when business hours resume.

19.2.4 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

20. Entire Agreement

20.1 The parties agree that the Contract and any documents entered into pursuant to it constitutes the entire agreement between them and supersedes all previous agreements, understandings and arrangements between them, whether in writing or oral in respect of its subject matter.

20.2 Each party acknowledges that it has not entered into the Contract or any documents entered into pursuant to it in reliance on, and shall have no remedies in respect of, any representation or warranty that is not expressly set out in the Contract or any documents entered into pursuant to it. No party shall have any claim for innocent or negligent misrepresentation on the basis of any statement in the Contract.

20.3 Nothing in these Conditions purports to limit or exclude any liability for fraud.

21. Variation

No variation of the Contract shall be valid or effective unless it is in writing, refers to the Contract and these Conditions and is duly signed or executed by, or on behalf of, Wightlink.

22. Assignment

22.1 The Supplier may not assign, subcontract or encumber any right or obligation under the Contract, in whole or in part, without Wightlink's prior written consent.

23. Set off

23.1 Wightlink shall be entitled to set-off under the Contract any liability which it has or any sums which it owes to the Supplier under the Contract or under any other contract which Wightlink has with the Supplier.

23.2 The Supplier shall pay all sums that it owes to Wightlink under the Contract without any set-off, counterclaim, deduction or withholding of any kind, save as may be required by law.

24. No Partnership or Agency

The parties are independent persons and are not partners, principal and agent or employer and employee and the Contract does not establish any joint venture, trust, fiduciary or other relationship between them, other than the

contractual relationship expressly provided for in it. None of the parties shall have, nor shall represent that they have, any authority to make any commitments on the other party's behalf.

25. Severance

25.1 If any provision of the Contract (or part of any provision) is or becomes illegal, invalid or unenforceable, the legality, validity and enforceability of any other provision of the Contract shall not be affected.

26. Conflicts within Contract

26.1 If there is a conflict between the terms contained in the Conditions and the terms of the Purchase Order, Schedules, appendices or annexes to the Contract, the terms of the Conditions shall prevail. The Supplier waives any right it might otherwise have to rely on any term endorsed upon, delivered with or contained in any documents of the Supplier that is inconsistent with these Conditions.

27. Third Party Rights

27.1 A person who is not a party to the Contract shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any of the provisions of the Contract.

28. Governing Law

The Contract and any dispute or claim arising out of, or in connection with, it, its subject matter or formation (including non-contractual disputes or claims) shall be governed by, and construed in accordance with, the laws of England and Wales.

29. Jurisdiction

The parties irrevocably agree that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of, or in connection with, the Contract, its subject matter or formation (including non-contractual disputes or claims).

Schedule 1

Code of Conduct

1. FORCED LABOUR

1.1 There shall be no forced, bonded, prison or compulsory labour in any form, or any form of human trafficking.

1.2 Suppliers shall ensure that workers, including migrant workers and workers supplied through an agency, are not required to make deposits, financial guarantees or payments to employers, labour providers, brokers or agencies to obtain work. Suppliers shall be responsible for payment of all fees and expenses.

1.3 Suppliers and, where relevant, workers' employers, labour providers or agencies shall not retain original copies of identity documents (such as passports, identity cards, work permits, bank books, ATM cards and other personal documents).

1.4 Suppliers shall not engage in making personal loans to workers or jobseekers under circumstances where repayment terms could be defined as debt bondage or forced labour.

1.5 Suppliers shall respect the right of workers to terminate their employment after reasonable notice and to receive all owed salary.

1.6 Suppliers shall respect the right of workers to leave the workplace after their shift. Where provided, workers' accommodation arrangements must not restrict workers' freedom of movement at any hour.

2. FREEDOM OF ASSOCIATION, COLLECTIVE BARGAINING AND WORKER CONSULTATION

2.1 Workers, without distinction, shall have the right to join or form trade unions of their own choosing and to bargain collectively.

2.2 Suppliers shall adopt an open attitude towards the activities of trade unions and their organisational activities.

2.3 Worker representatives shall not be discriminated against and shall have access to carry out their representative functions in the workplace.

2.4 Suppliers shall not use any form of physical or psychological violence, threats, intimidation, retaliation, harassment, or abuse against union representatives and workers seeking to form or join an organization of their own choosing.

2.5 Where the right to freedom of association and collective bargaining is restricted or prohibited by law, suppliers must not hinder workers from developing alternative mechanisms to express their grievances, protect their rights regarding working conditions and terms of employment, and negotiate their conditions, including pay. Suppliers must not seek to influence or control these mechanisms.

2.6 There is a clear and transparent system of worker and management communication that enables workers to consult and have an effective dialogue with management.

2.7 Suppliers shall provide a grievance mechanism for workers to raise workplace concerns. This grievance mechanism must involve an appropriate level of management and address concerns promptly, using an understandable and transparent process that provides timely feedback to those concerned, without any retribution. The mechanism must also allow for anonymous complaints to be raised and addressed. The existence and scope of this mechanism must be clearly communicated to all workers and their representatives, and all workers must have equal access.

2.8 Suppliers shall protect whistleblower confidentiality and prohibit retaliation.

3. HEALTH AND SAFETY

3.1 A safe and hygienic working environment shall be provided, bearing in mind the prevailing knowledge of the industry and any specific hazards. Adequate steps shall be taken to prevent accidents and injury to health arising out of, associated with, or occurring in the course of work, by minimising, so far as reasonably practicable, the causes of hazards inherent in the working environment.

3.2 Suppliers shall assign responsibility for health and safety to a senior management representative.

3.3 Workers shall receive regular and recorded health and safety training and such training shall be repeated for new or reassigned workers.

3.4 Male and female workers engaged in working with hazardous chemicals and materials will be informed of any potential risks to their reproductive health. To prevent unsafe exposure, appropriate arrangements shall be made for pregnant women.

3.5 Workers shall have access to clean toilet facilities, potable water, and sanitary facilities for food storage. The number of toilets within reasonable distance of the workplace required under applicable law shall be provided. The number of toilets shall also take into consideration the number of workers, privacy for each individual, and gender, accessibility, and hygiene. Undue restrictions shall not be imposed on the time and frequency of toilet use.

3.6 Accommodation, where provided, shall be clean, safe, and meet the basic needs of the workers.

3.7 Flexible working arrangements and on-site facilities shall be offered to women who are pregnant or nursing.

3.8 Workers shall have access to adequate health services in accordance with applicable national laws and international norms.

4. CHILD LABOUR

4.1 Suppliers must not employ any person under the age of 15 in any circumstances. In addition, suppliers shall not employ workers who are below either:

i) the legal minimum age for employment applicable to the Supplier; or

ii) the age of completion of compulsory education.

We consider all of the above to be children. Suppliers shall maintain robust age verification checks at all times to ensure they do not recruit or exploit children in any way.

4.2 If any child is found working directly or indirectly for the supplier, the Supplier shall implement a remediation plan, develop or participate in and contribute to policies and programmes that put the best interests of the child first, and provide for the transition of any such child to enable them to attend and remain in quality education until no longer a child.

4.3 Young workers under 18 years of age shall not be employed to work at night, or in conditions which compromise their health, safety, or moral integrity, or which harm their physical, mental, spiritual, moral or social development, or which interfere with their schooling or deprive them of the opportunity to attend school.

5. WAGES AND BENEFITS

5.1 Wages and benefits paid for a standard working week shall meet, as a minimum, national legal standards or industry benchmark standards, whichever is higher. In any event, wages shall always be enough to meet basic needs and to provide some discretionary income.

5.2 Suppliers shall work towards paying workers a fair living wage. Wages are essential for meeting the basic needs and expenditure of employees and reasonable savings. We seek business partners who progressively raise employee living standards through improved wage systems, benefits, welfare programmes and other services, which enhance quality of life.

5.3 Wages shall be paid regularly and on time.

5.4 Workers shall receive a payslip for each pay period, in a language they understand, clearly indicating the components of the compensation, including exact amounts for wages, benefits, incentives/bonuses and any deductions. Wage calculations shall be transparent, equitable and objective, including any for remuneration based on production, quotas, or piecework.

5.5 Female employees shall be entitled to maternity protection (leave and benefits as well as protection against discrimination) in accordance with the requirements of national laws and regulations, or International Labour Organisation Conventions Nos. 183, 103, and 3, whichever is the higher standard.

5.6 Deductions from wages as a disciplinary measure shall not be permitted nor shall any deductions from wages not provided for by national law without the express permission of the worker concerned. All disciplinary measures shall be recorded.

6. WORKING HOURS

6.1 Suppliers shall ensure that working hours comply with national laws, collective agreements, or benchmarked industry standards or relevant international standards, whichever affords greater protection to ensure the health, safety and welfare of workers. Working hours, excluding overtime, shall not exceed 48 hours per week. The total hours worked (including overtime) in any week shall not regularly exceed 60 hours in a single week.

6.2 Working hours may exceed 60 hours in a single week only in exceptional circumstances and where all of the following are met: this is permitted by national law; this is permitted by a collective agreement

freely negotiated with a workers' organisation representing a significant portion of the workforce; appropriate safeguards are taken to protect the worker's health and safety; and the employer can demonstrate that exceptional circumstances apply such as seasonal work, accidents or emergencies.

6.3 All overtime shall be voluntary.

6.4 Overtime shall be used responsibly and not be requested on a regular basis, taking into account the extent, frequency and hours worked by the individual worker and the workforce as a whole. It shall not exceed 12 hours per week and it shall not be used to replace regular employment. Overtime shall always be compensated at a premium rate, which is recommended to be not less than 125% of the regular rate of pay. Should a worker refuse to do overtime they shall not be punished, retaliated against, or penalised in any way.

6.5 Workers shall be provided with at least one day off in every 7 day period or, where permitted by national law, 2 days off in every 14 day period, as well as paid annual leave.

7. DISCRIMINATION

7.1 There is no discrimination in hiring, compensation, access to training, promotion, termination or retirement based on race, ethnic origin, caste, nationality, social , religion, age, disability, gender, marital status, family responsibilities, pregnancy status, sexual orientation, HIV/AIDs status, union membership or political affiliation.

7.2 Female workers shall be protected against threats of dismissal or any other employment decision that negatively affects their employment status in order to prevent them from getting married or becoming pregnant.

7.3 Suppliers shall not make use of pregnancy screening or testing at any time before or after the jobseeker signs an employment agreement, except where required by law. In such cases, the results of pregnancy screens or tests must only be used in accordance with the law.

8. EMPLOYMENT RELATIONSHIP

8.1 Work performed shall be on the basis of a recognised employment relationship established in compliance with national law and international labour standards.

8.2 All workers, both permanent and casual, shall be provided with clear written information and employment documents before they enter employment, containing accurate details of employment conditions, including pay, hours, overtime, benefits, leave, disciplinary and grievance systems. These documents shall be freely agreed, in a language that workers understand, and shall respect workers' legal and contractual rights.

8.3 Obligations to employees under labour or social security laws and regulations arising from the regular employment relationship shall not be avoided through the use of labour-only contracting, subcontracting, or home-working arrangements, or through apprenticeship schemes where there is no real intent to impart skills or provide regular employment. Nor shall any such obligations be

avoided through the excessive use of fixed-term contracts of employment.

9. HARASSMENT AND ABUSE

9.1 Suppliers shall commit to a workplace free of harassment and abuse. Physical and verbal abuse, physical discipline, and any other abuse, harassment or intimidation shall be prohibited, as shall the threat of any such abuse, harassment, or intimidation.

9.2 Sexual harassment, including unwelcome sexual advances, unwanted hugs and touches, suggestive or lewd remarks, requests for sexual favours, and the display of indecent, derogatory, or pornographic pictures, posters, drawings, or videos, shall be prohibited.

9.3 All workers, both men and women, shall be protected from retaliation for complaining about harassment and abuse.

10. ANTI-BRIBERY AND CORRUPTION

10.1 The offering, paying, soliciting or accepting of bribes or kickbacks, including facilitation payments, is strictly prohibited. General explanations for 'bribe' and 'facilitation payment' are included in the Appendix.

10.2 Suppliers, representatives and their employees must comply with all applicable anti-bribery and corruption laws. If no such anti-bribery or corruption laws apply or are of a lesser standard than that prescribed by the UK Bribery Act 2010, suppliers, representatives and their employees must adhere to the UK Bribery Act 2010.

10.3 Suppliers and representatives shall have in place anti-corruption and bribery procedures designed to prevent employees or persons associated with their business from committing offences of bribery or corruption. Suppliers and representatives will properly implement these procedures into their business and review them regularly to ensure that they are operating effectively.

11. ENVIRONMENTAL REQUIREMENTS

11.1 Suppliers shall support and encourage operating practices, farming practices and agricultural production systems that are sustainable.

11.2 Suppliers and their representatives shall continually strive towards improving efficiency and sustainability of their operations, which should include water conservation programmes.

11.3 Suppliers shall be able to demonstrate environmental management, including the following:

i) the Supplier should have a company environment representative;

ii) the Supplier should be aware of and be able to demonstrate compliance with all environmental legislation that may affect its activities;

iii) the Supplier should conduct an environmental review to determine whether any aspects of its operations, products or services can more fully reflect the requirements in this clause; and

iv) the Supplier should provide transparency in disclosing any enforcement, improvement or

prohibition notices served on its site(s) within the last three years.

12. LAND AND NATURAL RESOURCES

12.1 Suppliers shall adhere to the principle of free, prior and informed consent of all communities when acquiring land. The rights of communities and traditional peoples to maintain access to land, water and natural resources will be recognised and respected.

13. AUDIT AND TERMINATION OF AGREEMENTS

13.1 Suppliers shall only uses site(s) approved by Wightlink in writing and will not subcontract or change site(s) without Wightlink's further written approval.

13.2 Wightlink will provide guidance to Suppliers to help them understand our requirements and to implement policies and procedures to enable them to comply with our standards.

13.3 Compliance with this Code of Conduct is a mandatory requirement and will be subject to audit. Suppliers shall always demonstrate an open attitude to such audits, monitoring activities, visits and training programmes, including worker interviews, and give all cooperation to Wightlink Ovaltine's appointed auditors.

13.4 Where shortcomings with any aspect of this Code of Conduct are identified, the Supplier shall devise, and inform Wightlink of, its corrective action and implementation plans and timeline to effectively and promptly resolve the shortcomings.

13.5 Wightlink reserves the right to terminate an agreement with any supplier immediately for failure to comply with this Code of Conduct or where there is no willingness to make the appropriate changes.

14. COMPLIANCE WITH LAWS

14.1 Wightlink is fully committed to compliance with the applicable laws and regulations in each location where Wightlink conducts business, and will not knowingly operate in violation of any such law or regulation.

APPENDIX: Definitions

Bribe:

A bribe may involve giving or offering any form of gift, consideration, reward or advantage to someone in business or government in order to obtain or retain a commercial advantage or to induce or reward the recipient for acting improperly or where it would be improper for the recipient to accept the benefit. Bribery can also take place where the offer or giving of a bribe is made by or through a third party, e.g. an agent, representative or intermediary.

Some examples of bribes are as follows (this is not an exhaustive list): lavish gifts, meals, entertainment or travel expenses, particularly where they are disproportionate, frequent or provided in the context of ongoing business

negotiations; the uncompensated use of company services, facilities or property; cash payments; loans, loan guarantees or other credit; the provision of a benefit, such as an education scholarship or healthcare, to a member of the family of a potential customer/public or government official; providing a sub-contract to a person connected to someone involved in awarding the main contract; engaging a local company owned by a member of the family of a potential customer/public or government official; etc.

Facilitation Payment:

Facilitation payments are small payments or fees requested by government officials to speed up or facilitate the performance of routine government action (such as the provision of a visa or customs clearance). Such payments are strictly prohibited under this Code, regardless of whether they are permitted by national laws.

Schedule 2 – Data Processing

1. Definitions

In this agreement ("Agreement"), the following terms shall have the meanings set out below and be construed accordingly:

"Authorised Sub-Processors" means (a) those Sub-processors set out in Annex 3 (Sub-Processors); and (b) any additional Sub-processors consented to in writing by the Controller in accordance with Sub-Processing section.

"Controller Personal Data" means the data described in Annex 1 and any other Personal Data processed by a Processor on behalf of the Controller pursuant to or in connection with the relevant Contract.

"Erasure" means the removal or destruction of Personal Data such that it cannot be recovered or reconstructed.

"Third Country" means any country outside of the United Kingdom, except where that country is the subject of a valid adequacy decision by the United Kingdom on the protection of Personal Data in Third Country/ies.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Controller Personal Data transmitted, stored or otherwise processed.

"Process/Processing/Processed", "Data Controller", "Data Processor", "Data Subject", "Personal Data", "Special Categories of Personal Data" and any further definition not included under this Agreement shall have the same meaning as in Data Protection Laws.

"Services" means the services to be supplied by the Processor to the Controller pursuant to the relevant Contract.

"Sub-Processor" means any Data Processor (including any third party) appointed by the Processor to process Controller Personal Data on behalf of the Controller.

2. Data Processing Terms

2.1 In the course of providing the Services and/or products to the Controller pursuant to the Contract, the Processor may process Controller Personal Data on behalf of the Controller as per the terms of this Agreement. The Processor agrees to comply with the following provisions with respect to any Controller Personal Data. Wightlink as the Controller shall process the necessary Controller Personal Data to the Supplier as its Processor.

2.2 To the extent required by applicable Data Protection Laws, the Processor shall obtain and maintain all necessary licenses, authorisations and permits necessary to process Personal Data including Personal Data mentioned in Annex 1.

2.3 The Processor shall maintain all the technical and organisational measures to comply with the requirements set forth in this Agreement and its Annexes.

2.4 This Agreement shall start on the date of the Contract and shall continue for its duration unless either party terminates this Agreement.

3. Processing of Controller Personal Data

3.1 The Processor shall only Process Controller Personal Data for the purposes of this Agreement. The Processor shall not Process, transfer, modify, amend or alter the Controller Personal Data or disclose or permit the disclosure of the Controller Personal Data to any third party other than in accordance with Controller's documented instructions.

3.2 For the purposes set out in section 3.1 above, the Controller hereby instructs the Processor to transfer Controller Personal Data to the recipients in the Third Countries listed in Annex 3 (Sub-Processors), always provided that Processor shall comply with section 6 (Sub-Processing).

3.3 The Processor must comply promptly with any Controller's written instructions requiring the Processor to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised Processing.

4. Reliability and Non–Disclosure

4.1 The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Controller Personal Data, ensuring in each case that access is limited to those individuals who require access to the relevant Controller Personal Data to perform the Contract.

4.2 The Processor must ensure that all individuals which have a duty to process Controller Personal Data:

a) Are informed of the confidential nature of the Controller Personal Data and are aware of Processor's obligations under this Agreement in relation to the Controller Personal Data;
b) Have undertaken appropriate training/certifications in relation to the Data Protection Laws or any other training/certifications requested by Controller;
c) Are subject to confidentiality undertakings or professional or statutory obligations of confidentiality; and
d) Are subject to user authentication and logon processes when accessing the Controller Personal Data in accordance with this Agreement, and the applicable Data Protection Laws.

5. Personal Data Security

5.1 The Processor shall implement such measures considering the level of technical and organisational measures agreed by the parties, as appropriate as at the date of the Contract, having regard to the state of technological development and the cost of implementing such measures as set out in Annex 2 (Technical and Organisational Measures). The Supplier shall ensure a level of Controller Personal Data security appropriate to the risk, including but not limited to:

a) Pseudonymisation and encryption;
b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
c) The ability to restore the availability and access to Controller Personal Data in a timely manner in the event of a physical or technical incident; and
d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

5.2 The parties shall keep the security measures detailed in Annex 2 under review and shall carry out such updates as the Wightlink agrees are appropriate throughout the duration of this Agreement.

5.3 In assessing the appropriate level of security, the Processor shall consider the risks that are presented by Processing, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Controller Personal Data transmitted, stored or otherwise Processed and notify the Controller where required under applicable Data Protection Laws.

6. Sub-Processing

6.1 As of the date of the Contract, the Controller hereby authorises the Processor to engage those Sub-Processors set out in Annex 3 (Sub-Processors). The Processor shall not engage any Sub-Processors to Process Controller Personal Data other than with the prior written consent of the Controller, which the Controller may refuse with absolute discretion.

6.2 With respect to each Sub-Processor, the Processor shall:

a) Provide the Controller with full details of the Processing to be undertaken by each Sub-Processor.
b) Carry out adequate due diligence on each Sub-Processor to verify that it can provide an appropriate level of protection for the Controller Personal Data, including without limitation, sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of the UK GDPR, this Agreement and the applicable Data Protection Laws.
c) Include terms in the contract between the Processor and each Sub-Processor which are consistent as those set out in this Agreement. Upon request, the Processor shall provide a copy of its agreements with Sub-Processors to the Controller for its review.
d) Remain responsible for the acts and omissions of any such Sub-Processor as if they were the acts and omissions of the Processor.

6.3 As of the date of the Contract, the Controller hereby authorises the Processor to engage those Sub-Processors set out in Annex 3 (Sub-Processors).

7. Data Subject Rights

7.1 The Processor shall assist the Controller, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Laws with respect to security, breach notifications, impact assessments and consultations with any supervisory authorities or regulators.

7.2 The Processor shall promptly notify the Controller if it receives a request from a Data Subject, the supervisory authority and/or other competent authority under any applicable Data Protection Laws with respect to Controller Personal Data.

7.3 The Processor shall cooperate as requested by the Controller to enable the Controller to comply with any exercise of rights by a Data Subject under any Data Protection Laws with respect to Controller Personal Data and comply with any assessment, enquiry, notice or investigation under any Data Protection Laws with respect to Controller Personal Data or this Agreement, which shall include:

a) The provision of all data requested by the Controller within any reasonable timescale specified by the Controller in each case, including full details and copies of the complaint, communication or request and any Controller Personal Data it holds in relation to a Data Subject.
b) Where applicable, providing such assistance as is reasonably requested by the Controller to enable the Controller to comply with the relevant request within the timescales prescribed by the Data Protection Laws.
c) Implementing any additional technical and organisational measures as may be reasonably required by the Controller to allow the Controller to respond effectively to relevant complaints, communications or requests.

8. Personal Data Breach

8.1 The Processor shall notify the Controller without undue delay and, in any case, within twenty-four (24) hours upon becoming aware of or reasonably suspecting a Personal Data Breach. The Processor will provide the Controller with sufficient information as it has in its possession in respect of the Personal Data Breach. This should be submitted via email to the following:

Pennymanns@wightlink.co.uk

stuartjames@wightlink.co.uk

russellturner@wightlink.co.uk

Such notification shall as a minimum:

a) Describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;
b) Communicate the name and contact details of the Processor's data protection officer / privacy officer or other relevant contact from whom more information may be obtained; and
c) Describe the measures taken or proposed to be taken to address the Personal Data Breach.

8.2 The Processor shall co-operate with the Controller and take such reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each Personal Data Breach. Immediately following any accidental, unauthorised or unlawful Personal Data Processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Processor will reasonably co-operate with the Controller at no additional cost to the Controller, in the Controller's handling of the matter, including but not limited to:

(a) assisting with any investigation;
(b) providing the Controller with physical access to any facilities and operations affected;
(c) facilitating interviews with the Processor's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;
(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Laws or as otherwise reasonably required by the Controller; and
(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data Processing.

8.3 In the event of a Personal Data Breach, the Processor shall not inform any third party without first obtaining the Controller's prior written consent, unless notification is required by the laws of the United Kingdom or supervisory authority, in which case the Processor shall, to the extent permitted and to the extent that time allows, inform the Controller of that legal requirement, provide a copy of the proposed notification and consider any prompt and reasonable comments made by the Controller before notifying the Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

9.1 Upon request by the Controller, the Processor shall provide reasonable assistance to the Controller with any data protection impact assessments which are required under Article 35 of the UK GDPR and with any prior consultations to any supervisory authority of the Controller which are required under Article 36 of the UK GDPR, in each case solely in relation to Processing of Controller Personal Data by the Processor on behalf of the Controller and considering the nature of the Processing and information available to the Processor.

10. Erasure or return of Controller Personal Data

10.1 Processor shall promptly and, in any event, within 90 (ninety) calendar days of the earlier of:

(i) cessation of Processing of Controller Personal Data by Processor; or

(ii) termination of this Agreement, at the choice of Controller (such choice to be notified to Processor in writing) either:

a) Return a complete copy of all Controller Personal Data held by the Processor and its Sub-Processors (which the Controller doesn't have a copy of) to the Controller by secure file transfer in such format as notified by the Controller to the Processor and securely erase all other copies of Controller Personal Data Processed by the Processor or any Authorised Sub-Processor; or
b) Securely delete all copies of Controller Personal Data Processed by Processor or any Authorised Sub-Processor, and in each case, provide a written certification to the Controller that it has complied fully with such requirements.

10.2 Notwithstanding the provision of clause 10.1, the Processor may retain Controller Personal Data to the extent required by the applicable laws, but only to the extent and for such period as required by the applicable law, and always provided that the Processor shall ensure the confidentiality of all such Controller Personal Data and shall ensure that such Controller Personal Data is only Processed as necessary for the purpose(s) of applicable laws requiring its storage and for no other purpose.

11. Audit rights

11.1 The Processor shall make available to the Controller, upon written request and at reasonable notice, such information as is in its possession and as is reasonably necessary to demonstrate the Processor's compliance with this Schedule and allow for, and contribute to audits, including inspections by the Controller or another auditor mandated by the Controller of any premises where the Processing of Controller Personal Data takes place. This may include, but is not limited to:

a) physical access to, remote electronic access to, and copies of the records and any other information held at the Processor's premises or on systems storing the Personal Data;
b) access to and meetings with any of the Processor's personnel reasonably necessary to provide all explanations and perform the audit effectively; and
c) inspection of all records and the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process the Personal Data.

11.2 The Processor shall permit the Controller, or another auditor mandated by the Controller to inspect, audit and copy any relevant records, processes and systems in order that the Controller may satisfy itself that the provisions of this Agreement are being complied with.

11.3 The Processor shall provide full cooperation to the Controller with respect to any such audit and shall, at the request of the Controller, provide the Controller with evidence of compliance with its obligations under this Agreement.

11.4 The Processor shall immediately inform the Controller if, in its opinion, an instruction pursuant to this paragraph (Audit rights) infringes the Data Protection Laws.

11.5 If a Personal Data Breach occurs or is occurring, or the Processor becomes aware of a breach of any of its obligations under this Agreement or any Data Protection Laws, the Processor will:

a. promptly, conduct its own audit to determine the cause;
b. produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;
c. provide the Controller with a copy of the written audit report; and
d. remedy any deficiencies identified by the audit within 7 days.

11.6 At the Controller's written request, the Processor will:

(a) conduct an information security audit before it first begins processing any of the Personal Data and repeat that audit on at least an annual basis at the Processor's own cost;
(b) produce a written report that includes detailed plans to remedy any security deficiencies identified by the audit;
(c) provide the Controller with a copy of the written audit report; and
(d) remedy any deficiencies identified by the audit within 7 days.

12. International Transfers of Controller Personal Data

12.1 Processor shall not process Controller Personal Data nor permit any Authorised Sub-Processor to process the Controller Personal Data in a Third Country, other than with respect to those recipients in Third Countries (if any) listed in Annex 3 (Sub-Processors), unless authorised in writing by Controller in advance, via an amendment to this Agreement.

13. Codes of Conduct and Certification

13.1 At the request of the Controller, the Processor shall comply with any Code of Conduct approved pursuant to Article 40 of the UK GDPR and obtain any certification approved by Article 42 of the UK GDPR, to the extent that they relate to the Processing of Controller Personal Data.

14. Indemnification

14.1 The Processor shall indemnify and keep indemnified the Controller against all losses, claims, damages, liabilities, fines, sanctions, interest, penalties, costs, charges, expenses, compensation paid to any third party, demands and legal and other professional costs (calculated on a full indemnity basis and in each case whether or not arising from any investigation by, or imposed by, a supervisory authority) arising out of or in connection with any Personal Data Breach by the Processor, any breach by the Processor of its obligations under this Agreement or the Processor's breach of the Data Protection Laws.

14.2 This Clause 14 shall survive termination of this Agreement.

15. Warranties

15.1 The Processor warrants and represents that:

(a) its employees, subcontractors, agents and any other person or persons accessing the Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Law;

(b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Laws enactments, regulations, orders, standards and other similar instruments;

(c) it has no reason to believe that the Data Protection Laws prevent it from providing any of the contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the unauthorised or unlawful Processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

(i) the harm that might result from such unauthorised or unlawful Processing or accidental loss, destruction or damage;

(ii) the nature of the Personal Data protected; and

(iii) comply with all applicable Data Protection Laws and its information and security policies, including the security measures required in Clause 5.1 of this Schedule 2 .

15.2 The Controller warrants and represents that the Processor's expected use of the Personal Data for the business purposes and as specifically instructed by the Controller will comply with the Data Protection Laws.

16. General Terms

16.1. Subject to this section, the parties agree that this Agreement will remain in full force and survive any termination or expiration of this Agreement.

16.2. Neither the Processor nor any Sub-Processor is obliged to undertake any unlawful transfer or Processing of Controller's Personal Data and shall not be liable to the extent that it (or any Sub-Processor) is delayed in or fails to perform any obligation under this Agreement due to it (or any Sub-Processor) being unable (or reasonably believing it is unable) to undertake any transfer or Processing in a lawful manner.

16.3 The Processor must notify the Controller immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the Processing of the Personal Data or to either party's compliance with the Data Protection Laws.

ANNEX 1: DETAILS OF PROCESSING OF CONTROLLER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Controller Personal Data as required by Article 28(3) of the UK GDPR.

Subject matter and duration of the Processing of Controller Personal Data

The subject matter and duration of the Processing of the Controller Personal Data are set out in this Agreement.

The nature and purpose of the Processing of Controller Personal Data

xxxxxxxxxxxxxxx

The types of Controller Personal Data to be processed

Xxxxx

The categories of Data Subject to whom the Controller Personal Data relates

xxxxxxx

ANNEX 2: TECHNICAL AND ORGANISATIONAL MEASURES

Organisational security measures

1.Security Management

Security policy and procedures: The Processor must have a documented security policy with regard to the Processing of personal data which covers the below:

1) Roles and responsibilities related to the Processing of personal data is clearly defined and allocated in accordance with the security policy.
2) During internal re-organisations or terminations and change of employment, revocation of rights and responsibilities with respective hand-over procedures is clearly defined.
3) Access Control Policy: Specific access control rights are allocated to each role involved in the Processing of Personal Data, following the need-to-know principle.
4) Resource/asset management: Processor has a register of the IT resources used for the Processing of personal data. A specific person is assigned the task of maintaining and updating the relevant data protection register (e.g. IT officer).
5) Change management: Processor makes sure that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process must take place.

2.Incident response and business continuity

Incident's handling / Personal Data Breaches:

1) An incident response plan with detailed procedures is defined to ensure effective and orderly response to incidents pertaining Personal Data.
2) Processor will report without undue delay to the Controller any security incident that has resulted in a loss, misuse or unauthorised acquisition of any personal data.
3) Business continuity: Processor establishes the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system Processing personal data (in the event of an incident/Personal Data Breach).

3.Human resources

1) Confidentiality of personnel: The Processor ensures that all employees understand their responsibilities and obligations related to the Processing of Personal Data. Roles and responsibilities are clearly communicated during the pre-employment and/or induction process.
2) Training: The Processor ensures that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the Processing of Personal Data are also properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.

4.Technical security measures

Access control and authentication:

1) An access control system applicable to all users accessing the IT system is implemented. The system allows creating, approving, reviewing and deleting user accounts.
2) The use of common user accounts is avoided. In cases where this is necessary, it is ensured that all users of the common account have the same roles and responsibilities.

3) When granting access or assigning user roles, the "principle of least privilege" shall be observed in order to limit the number of users having access to personal data only to those who require it for achieving the Processor's Processing purposes.
4) Where authentication mechanisms are based on passwords, the Processor requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability.
5) The authentication credentials (such as user ID and password) shall never be transmitted unprotected over the network.
6) Logging and monitoring: Log files are activated for each system/application used for the Processing of Personal Data. They include all types of access to data (view, modification, deletion).

5.Security of data at rest

Server/Database security:

1) Database and applications servers are configured to run using a separate account, with minimum privileges to function correctly.
2) Database and applications servers only process the Personal Data that are actually needed to process in order to achieve its Processing purposes.
3) All data is encrypted in transit and at rest.

6.Workstation security:

1) Anti-virus applications and detection signatures is configured on a regular basis.
2) The Processor maintains a clear desk / clear screen policy.

7.Network/Communication security:

1) Whenever access is performed through the internet, communication is encrypted through cryptographic protocols.
2) Traffic to and from the IT system is monitored and controlled through firewalls and intrusion detection systems.

8.Back-ups:

1) Backup and data restore procedures are defined, documented and clearly linked to roles and responsibilities.
2) Backups are given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.
3) Execution of backups is monitored to ensure completeness.

9.Mobile/Portable devices:

1) Mobile and portable device management procedures are defined and documented establishing clear rules for their proper use.

10. Application lifecycle security:

1) During the development lifecycle a secure development policy is followed.

11. Physical security:

1) The physical perimeter of the IT system infrastructure is not accessible by non-authorised personnel. Appropriate technical measures and organisational measures shall be set in place to protect security areas and their access points against entry by unauthorised persons.

ANNEX 3: SUB-PROCESSORS

The Authorised Sub-Processors for the purpose of this Agreement are (including delegates who process client personal data):

Supplier Name	Nature of Supply or Services	Does the supplier process personal data?	Third Country location

Schedule 3 – IT Security

For the purposes of this Schedule, the following terms have the following meanings:

Customer Information Security Policy or Policy means this policy as set out in this Schedule, as may be amended by Wightlink from time to time.

Information Security Program means a program designed and maintained by the Supplier to protect the Wightlink Information it receives, processes, transfers, transmits, stores, delivers and/or otherwise accesses.

Relevant Personnel means all Supplier personnel or third parties that have or may have access to a Resource, the Wightlink Network and/or Wightlink Information.

Resource means all Supplier devices, including laptops, personal computers, routers, servers and other computer systems that store, process, transfer, transmit, deliver or otherwise access Wightlink Information.

Wightlink Information means Wightlink's data files, databases, applications, software (source code and object code), software documentation, supporting process documents, operational process and procedure documentation, test plans, test cases, test scenarios, cyber incident reports and any other Confidential Information belonging to Wightlink.

Wightlink Network means the network belonging to or hosted on behalf of Wightlink.

Purpose

This Schedule sets out the security requirements to which the Supplier must adhere in order to protect Wightlink Information.

Security Requirements

1. Information Stewardship - The Supplier will identify a named individual responsible for information security. This role will have overall responsibility to ensure compliance with the Supplier's security controls, including the maintenance of equipment and patch level, to support the confidentiality, availability and integrity of Wightlink Information.

2. Confidentiality and Integrity - The Supplier will utilise a managed approach to security to ensure that Wightlink Information is protected through its entire life cycle, from creation, transformation, use, storage and destruction, regardless of the storage media (for example, tape, disk or paper).

3. Vulnerability Management - Where the Supplier is processing Wightlink data or accessing Wightlink systems the Supplier will:

    (a) keep its firewalls, routers, servers, personal computers and all other Resources current with appropriate security-specific system patches and other updates, which have been tested prior to installation;

    (b) perform regular tests (including patch management, port scanning and virus scanning) of its Resources to detect any known vulnerabilities;

(c) address critical and high-risk vulnerabilities within five days of identification and other less critical vulnerabilities within a reasonable time-frame;

(d) Remove unnecessary services and update other configurations on Resources that may subject the Resources to unnecessary risk; and

(e) procure, at least once in every twelve-month period, an independent third party to perform penetration tests to assess the Resources.

4. Logging and Monitoring

(a) Maintain and monitor relevant logs to detect potentially malicious activity on systems used to access or process Wightlink data. This should include:

i. All attempts (successful and unsuccessful) to access Wightlink Information or systems that support delivery of the service; and

ii. Logs from relevant security systems used to protect Wightlink Information, or systems used to process Wightlink information or access Wightlink systems; and

iii. retain such audit logs in a protected state (encrypted or locked) for at least 90 days;

5. Intrusion Detection and Prevention

(a) The Supplier will use security measures to protect against network intrusions, malicious software or system compromise that could affect the Supplier's telecommunications system and any computer system or network device that the Supplier uses to provide the Services.

(b) The Supplier will establish documented processes and procedures for responding to security violations, suspicious events and incidents. When events require an investigative response, the Supplier will maintain a thorough "case file" for Wightlink's benefit whenever Wightlink Information is at risk.

(c) The Supplier will inform Wightlink of confirmed security violations or incidents that impact Wightlink as soon as practical and within forty-eight (48) hours of the Supplier becoming aware of such violation or incident.

6. Malware Defence

(a) The Supplier will, in relation to the Resources:

i. implement and maintain an up-to-date commercially available computer virus detection/scanning program on any Resources used to process Wightlink Information or access Wightlink's systems;

ii. install and use such computer virus detection/scanning on all data sending mechanisms as well as at any other points directed by Wightlink; and

iii. keep all anti-virus software up-to-date by installing new definition files when made available by the Supplier's anti-virus vendor.

7. Encryption and PKI

(a) The Supplier will ensure that all Wightlink Information classified as "Wightlink Confidential" or "Restricted" is encrypted when in storage.

8. Network Security

(a) The Supplier shall:

i. implement and maintain strong, industry standard encryption techniques for all cases in which data identified as Wightlink are transmitted over any public data network;

ii. ensure that its internet connections are protected with dedicated, industry-recognised firewalls that are configured and managed in accordance with industry-recognised standards and that no internal or private internet protocol addresses will be publicly available or natively routed to the internet; and

iii. ensure that screen savers with password protection engage after 15 minutes of inactivity on any laptop or desktop computer on which Wightlink Information is stored or through which Wightlink Information can be accessed.

(b) Where the Supplier is given access to the Wightlink Network, the Supplier will:

i. not access or attempt to access any information, data or materials contained on the Wightlink Network other than those necessary for the performance of its obligations to Wightlink;

ii. restrict such access to those employees, officers, representatives or agents who have been given accounts by Wightlink;

iii. fully comply with any security guidelines or other rules in respect of access to and use of such network as notified to the Supplier by Wightlink; and

iv. agree acceptable methods of connectivity with Wightlink on an individual project basis, using one of the standard approaches allowed by Wightlink.

9. Identification, Authentication and Authorisation

(a) The Supplier shall:

i. ensure that all Relevant Personnel are uniquely identified to and authenticated by the Resource and the Supplier will not use any form of generic or shared user identifier to access Wightlink Information without agreement from Wightlink;

ii. ensure that the level of authentication required for access to any Resource is proportionate to the classification of Wightlink Information stored on or processed by the Resource;

iii. ensure that access to privileged accounts will be restricted to only those people who administer the relevant Resource and individual accountability will be maintained;

iv. ensure that the default password (such as those from hardware or software vendors) for any Resource will be changed immediately upon receipt of that Resource by the Supplier;

v. enforce the principle of "least privilege", namely, that Staff only have the level of access to Resources required to perform their job functions in relation to the Resource and have such rights and privileges for the shortest length of time necessary;

vi. remove the physical and logical access rights of any Relevant Personnel to Wightlink Information immediately upon such Relevant Personnel's termination or transfer;

vii. destroy all Wightlink Information from any media, whether hard copy, magnetic, optical or any other form, before disposing of such media. Such destruction may be carried out on or about the premises by assigned Relevant Personnel using commercially available shredding devices or software, or by a reputable third-party shredding service; and

viii. Where the Supplier grants Wightlink access to the Supplier's system, the Supplier shall ensure that access privileges in that system allow for role-based access control, i.e. access profiles determined by job functions, and must comply with the need-to-know / need-to-have concept.

10. User Passwords and Accounts

(a) The Supplier will ensure that access to the Resources is authenticated by passwords or multi-factor authentication. Where passwords are used they should meet industry best-practice recommendations on password length, complexity and expiry and be encrypted in storage and transmission.

11. Third Party Relationships

(a) The Supplier shall:

i. not use new third party resources without the prior written approval of Wightlink; and

ii. conduct security risk assessments of any third party service providers with access to Wightlink Information and ensure that such subcontractors have in place (and are contractually obliged to maintain) procedures and safeguards at least as stringent as the procedures and safeguards described in this Schedule.

12. Remote Access Connection Authorisation

(a) Where the Supplier provides remote access to systems used to store, process access Wightlink Information the Supplier will:

i. ensure all remote access connections to the Supplier's internal networks and/or computer systems require authorisation and that the authorisation is regularly reviewed to ensure it remains accurate; and

ii. provide an industry standard means of access control at the "point of entry" to the Supplier computing or communication resources through multi-factor authentication, which uses secure access channels, such as a virtual private network.

13. Secure System Development

(a) Where the Supplier is developing systems for Wightlink the Supplier will ensure that:

i. all software applications it develops for Wightlink follow a secure Systems Development Life Cycle (SDLC) methodology;

ii. applications are deployed in a secure production environment;

iii. where test environments are to contain Wightlink Information, the Supplier shall ensure that access controls are equivalent to those required in a live production environment; and

iv. where test environments contain Personal Data, this information should, when possible, be anonymised or sanitised so that data is not attributable to any individual. Where this is not possible, the Supplier shall comply with all applicable laws and the terms of this Agreement in the handling of such Personal Data.

14. Personnel Security

(a) The Supplier must perform background checks on the Relevant Personnel prior to granting such Relevant Personnel access to a Resource. As a minimum, such checks must include:

i. identity verification;

ii. verification of employment references; and

iii. confirmation of applicable qualifications.

(b) Where local laws allow, Wightlink may require the Supplier to perform additional screening of Relevant Personnel in its absolute discretion, including financial checks or criminal record bureau checks.

15. Training and Awareness

(a) The Supplier will require all Relevant Personnel to participate in training and awareness sessions at least annually in respect of the processes and procedures set out in this Schedule and will track attendance and provide testing to ensure training materials are understood.

16. Business Continuity

(a) The Supplier will implement and maintain a business continuity plan that includes:

i. a recovery strategy and procedures;

ii. estimated recovery time for products and services; and

iii. a procedure for notifying Wightlink.

(b) The Supplier will test its business continuity plan as often as required (but no less than every six months) to reasonably ensure a successful recovery in the event an actual recovery is required.

(c) Wightlink's role in the business continuity plan must be clearly defined.

(d) Wightlink reserves the right to directly participate in the recovery tests as well as to audit, with appropriate notice, the plans and test results on a regular basis.

(e) The Supplier shall provide Wightlink with a copy of the business continuity plan upon reasonable request.

17. Contract Termination and Data Retrieval / Removal

(a) Upon termination of the Agreement between the Supplier and Wightlink, the Supplier shall promptly return, or procure the return of the Wightlink Information in a format and on media reasonably requested by Wightlink or at Wightlink's request destroy the same and provide Wightlink with written confirmation that the Wightlink Information has been destroyed.

18. Suspension of access

(a) The Supplier shall immediately inform Wightlink on becoming aware that Wightlink Information has been disclosed or if the Supplier's own network has been accessed or used in a way which breaches of the terms of this Policy. The Supplier shall promptly provide Wightlink with the details of any such disclosure, access or use and shall provide Wightlink with such assistance as Wightlink may reasonably require in order to investigate, prevent or remedy any such disclosure, access or use.

(b) Wightlink shall be entitled to suspend the Supplier's access to the Wightlink Network if it reasonably believes a suspension of access is required in order to prevent or cease any breach of this Policy or in case of any actual, attempted or suspected unauthorised access or use of the Wightlink Network.

(c) Any suspension of access undertaken as a result of the Supplier's negligence, unlawful act or omission or breach of this Policy shall not relieve the Supplier of its obligations under its agreement(s) with Wightlink.

19. Compliance and Audit

(a) The Supplier should provide WIGHTLINK with independent evidence, either through recognised external certification or an audit by a mutually agreed third-party, that the Supplier's operations and controls meet the security requirements described in this Schedule.

(b) Up to twice a year and with at least 8 weeks' notice, Wightlink may conduct audits and onsite security control assessments of the Supplier's compliance with this Schedule. The Supplier will make its managers and senior technicians available to assist with any such audits.

ANNEX 1: TECHNICAL AND ORGANISATIONAL MEASURES

Organisational security measures

1. Security Management

Security policy and procedures: The Processor must document a security policy with regard to the processing of Personal Data.

1) Roles and responsibilities related to the processing of Personal Data is clearly defined and allocated in accordance with the security policy.
2) During internal re-organisations or terminations and change of employment, revocation of rights and responsibilities with respective hand-over procedures are clearly defined.
3) Access Control Policy: Specific access control rights are allocated to each role involved in the processing of Personal Data, following the need-to-know principle.

4) Resource/asset management: The Processor has a register of the IT resources used for the processing of Personal Data. A specific person is assigned the task of maintaining and updating the register (e.g. IT officer).
5) Change management: The Processor makes sure that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process takes place.

2.Incident response and business continuity

Incident's handling / Personal Data breaches:

1) An incident response plan with detailed procedures is defined to ensure effective and orderly response to incidents pertaining Personal Data.
2) The Processor will report without undue delay to the Controller any security incident that has resulted in a loss, misuse or unauthorised acquisition of any personal data.
3) Business continuity: The Processor establishes the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing Personal Data (in the event of an incident/Personal Data Breach).

3.Human resources

1) Confidentiality of personnel: The Processor ensures that all employees understand their responsibilities and obligations related to the processing of Personal Data. Roles and responsibilities are clearly communicated during the pre-employment and/or induction process.
2) Training: The Processor ensures that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of Personal Data are also properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns and training.

4.Technical security measures

Access control and authentication:

1) An access control system applicable to all users accessing the IT system is implemented. The system allows creating, approving, reviewing and deleting user accounts.
2) The use of common user accounts is avoided. In cases where this is necessary, it is ensured that all users of the common account have the same roles and responsibilities.
3) When granting access or assigning user roles, the "principle of least privilege" shall be observed in order to limit the number of users having access to Personal Data only to those who require it for achieving the Processor's processing purposes.
4) Where authentication mechanisms are based on passwords, the Processor requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability.
5) The authentication credentials (such as user ID and password) shall never be transmitted unprotected over the network.
6) Logging and monitoring: Log files are activated for each system/application used for the processing of Personal Data. They include all types of access to data (view, modification, deletion).

5.Security of data at rest

Server/Database security:

1) Database and applications servers are configured to run using a separate account, with minimum privileges to function correctly.
2) Database and applications servers only process the Personal Data that are actually needed to process in order to achieve its processing purposes.
3) All data is encrypted in transit and at rest.

6.Workstation security:

1) Anti-virus applications and detection signatures is configured on a regular basis.
2) The Processor maintains a clear desk / clear screen policy.

7.Network/Communication security:

1) Whenever access is performed through the internet, communication is encrypted through cryptographic protocols.
2) Traffic to and from the IT system is monitored and controlled through firewalls and intrusion detection systems.

8.Back-ups:

1) Backup and data restore procedures are defined, documented and clearly linked to roles and responsibilities.
2) Backups are given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.
3) Execution of backups is monitored to ensure completeness.

9.Mobile/Portable devices:

1) Mobile and portable device management procedures are defined and documented establishing clear rules for their proper use.

10. Application lifecycle security:

1) During the development lifecycle a secure development policy is followed.

11. Physical security:

1) The physical perimeter of the IT system infrastructure is not accessible by non-authorised personnel. Appropriate technical measures and organisational measures shall be set in place to protect security areas and their access points against entry by unauthorised persons.

SIGNED by ..... *(name)*

..... *(signature)*

duly authorised for and on behalf of

WIGHTLINK LIMITED

SIGNED by ..... *(name)*

..... *(signature)*

duly authorised for and on behalf of

[INSERT SUPPLIER NAME]