VIRGIN MEDIA PURCHASE ORDER TERMS AND CONDITIONS

1. Delivery.

1.1. The date of delivery of Products and the provision of any Services shall be as specified in the Purchase Order.

1.2. If the Supplier is late with any delivery of Products or provision of any Services Virgin Media shall have the right to terminate the Purchase Order (without liability to Virgin Media) at any time before delivery of the Products or provision of the Services and, if set out in the Purchase Order, Virgin Media shall be entitled to receive payment of liquidated damages.

1.3. The Products shall be delivered by the Supplier at its cost and risk to the address specified in the Purchase Order.

1.4. The Supplier shall repair or replace free of charge any Products damaged or lost in transit and due delivery of the Products shall not be deemed to have taken place until the replacement Products have been delivered. Virgin Media reserves the right to hold such damaged Products at the Supplier's risk or to return them at the risk and expense of the Supplier.

1.8 The Supplier shall provide reasonable advice, co-operation or assistance in connection with Virgin Media's enjoyment of use of Products, Deliverables or Services provided under the Purchase Order.

2. Acceptance.

2.1 The Supplier shall allow Virgin Media to inspect and/or test the Products or Deliverables or work before giving acceptance.

2.2 Following the inspection and/or testing of the Products, Deliverables or work Virgin Media shall be entitled to reject any Products, Deliverables or work which do not comply with the standard required or the terms expressed or implied in the Purchase Order as to quality, quantity, condition, fitness for purpose, description or otherwise. Products or Deliverables so rejected, unless collected by the Supplier, will be returned at the Supplier's expense and risk.

3. Work on Virgin Media's Premises.

Where any Purchase Order involves work being carried out on or delivery at Virgin Media's premises the Supplier and its employees, agents and sub-contractors shall observe all statutory rules and regulations and all of Virgin Media's applicable policies, rules and regulations. Virgin Media may (at its sole discretion) refuse to admit or may order the removal of any person who in its reasonable opinion is not fit to be on the premises.

4. Price.

4.1. The price of the Products and the Services shall be as stated in Purchase Order and, unless otherwise so stated, shall be: (a) exclusive of any applicable UK value added tax; and (b) inclusive of all other charges and costs (including of packaging, packing, shipping, carriage, insurance and delivery) and of any duties, taxes or levies other than UK value added tax; and (c) full and exclusive remuneration of the Supplier for performance of its obligations under the Purchase Order.

4.2. No increase in the price may be made (whether on account of additional effort, additional or increased material, labour or transport costs, fluctuation in rate of exchange or otherwise) without the Parties' prior agreement in writing.

4.3. Payment of the undisputed price shall be made within ninety (90) days of receipt of the Supplier's invoice, unless otherwise agreed by the Parties in writing.

4.4. Virgin Media shall be entitled to set off against the price any undisputed sums owed to Virgin Media by the Supplier.

4.5. The defaulting party shall pay to the other (if demanded) interest on any undisputed amount outstanding at the rate of 1% per annum above the base rate of National Westminster Bank plc, for the period from the due date until the date of actual payment.

4.6. The Supplier shall not issue any invoice sixty (60) days after the end of the period in which the charges were incurred.

5. Title.

Property in the Products shall pass to Virgin Media on the earlier of delivery or payment of the purchase price.

6. Software Licence.

The Supplier grants to Virgin Media a non-exclusive, royalty free, perpetual and irrevocable right to use any software supplied (together with any updates or new versions to that software) and any associated materials for such purposes as Virgin Media may require and, where relevant, to sub-license any such item to Virgin Media's customers for the purpose of accessing and using Virgin Media`s services. Virgin Media shall not make any copies or duplicates of any such item (unless reasonably necessary to do so for the above purposes) without the Supplier's prior written consent, save for backup and archival purposes.

7. Warranty, Indemnity and Liability.

7.1. The Supplier warrants, represents and undertakes to Virgin Media that (without prejudice to Virgin Media's rights and remedies implied by statute and common law):

(a) the Supplier has the corporate power and authority to execute, deliver and perform its obligations under the Purchase Order and has the right to and shall supply all Products and Deliverables free from any charges, liens or other encumbrances;

(b) all Products, Deliverables and Services shall correspond with description and other specification supplied or made known to the Supplier and with any sample and comply with all current and applicable laws and regulatory requirements;

(c) the Products and Deliverables will be free from defects in design, material, workmanship and performance and will not contain or introduce to any equipment or system any computer viruses, trojan horses or other destructive, disruptive or nuisance computer programs; and

(d) Virgin Media`s receipt, possession and/or use of the Products, Services and Deliverables provided by the Supplier (or its subcontractor) shall not infringe any Intellectual Property Rights of any person.

7.3. Nothing in this Purchase Order excludes or limits:

(a) a party's liability to the other party for fraud or for death or personal injury due to its own negligence or its employees' or agents'

negligence whilst acting in the course of their employment;

(b) the Supplier's liability under Clause 11 (Confidentiality) or Clause 12 (IT Security, Virgin Media Data and Data Security, and Data Protection) or under the indemnity given by it in Clause 10.4 (Intellectual Property) and Clause 13.14.

7.4. Subject always to the provisions of Clause 7.3, neither party shall be liable to the other for any type of special, indirect or consequential loss including, without limitation, any loss of profit or anticipated savings.

7.5. (a) Subject always to the provisions of Clause 7.3, the Supplier's liability to Virgin Media, whether in contact or tort (including negligence), for breach of statutory duty, or otherwise, arising under or in connection with the Purchase Order shall not exceed in the aggregate the greater of £1 million or 200% (two hundred percent) of the total amounts paid or payable by Virgin Media to the Supplier under the Purchase Order;

(b) Subject to Clause 7.3, Virgin Media's liability to the Supplier (or its affiliates) whether in contract or tort (including negligence), for breach of statutory duty, or otherwise, arising under or in connection with this Purchase Order shall not exceed 100% (one hundred percent) of the total amounts paid or payable by Virgin Media to the Supplier under the Purchase Order.

7.6 The Supplier will at all times maintain insurance with a reputable insurance company against all liability under the Purchase Order and shall provide reasonable evidence of such insurance to Virgin Media on request.

8. Remedy.

Without prejudice to any other remedy, if any Products, Deliverables or Services are not supplied or performed in accordance with the Purchase Order, then Virgin Media shall be entitled to require the Supplier to repair the Products, Deliverables or to supply replacement Products, Deliverables or Services in accordance with the Purchase Order within 7 days or to have them so repaired or re-performed by a third party in which case the Supplier shall reimburse Virgin Media for all costs and expenses thereby incurred.

9. Termination.

9.1. Either party may terminate the Purchase Order without liability immediately upon notice in writing to the other party if the other party at any time shall become insolvent or become the subject of a winding up order (of any type) or an administration order, or have an administrative receiver appointed (including under the Law of Property Act), or compound with its creditors, enter into a company voluntary arrangement or scheme of arrangement (in any such case other than in connection with liquidation a reconstruction or amalgamation) or is subject to an event that has the equivalent or similar effect to any of the aforementioned events.

9.2. Either party may terminate the Purchase Order immediately upon written notice to the other at any time for material breach (i) not capable of remedy, or (ii) if the breach is capable of remedy, it is not remedied within twenty (20) days of written notice to remedy the same.

9.3. Virgin Media may terminate the Purchase Order at any time by giving not less than thirty (30) days written notice to the Supplier, without liability.

9.4. On termination or expiry of the Purchase Order, the Supplier shall return all information or materials made available by or on behalf of Virgin Media to the Supplier and shall co-operate fully with Virgin Media to ensure an orderly, efficient and undisruptive as reasonably possible transfer of the Supplier's obligations to Virgin Media (or its nominated third party).

10. Intellectual Property.

10.1. Neither Party shall acquire any rights to any pre-existing Intellectual Property owned by the other Party and/or its licensors.

10.2. Unless otherwise agreed in writing, all copyright and other intellectual property rights in any goods, products, materials, software, drawing, reports or other documents or data generated, created or produced by the Supplier in the performance of the Agreement (including all future rights arising out of such items and any preparatory material) (the "Works") and physical possession of any media upon which such Works are contained shall vest in and be the property of and are hereby assigned to the Virgin Media. The Supplier hereby waives all moral rights in the Works, and confirms that it has obtained all waivers of moral rights and consents from any agent or sub-contractor or other third party necessary to comply with its obligations hereunder.

10.3 Where the intellectual property rights in any Works have not, for whatever reason, been assigned to Virgin Media, the Supplier hereby grants to Virgin Media and all other Virgin Media group companies an exclusive, perpetual, irrevocable, royalty-free licence to use, copy or modify the Works with a right to sub-license those Works to third parties. The Supplier agrees to promptly deliver up all copies of the Works and associated materials necessary for the use of the Works to Virgin Media on demand.

10.4 The Supplier shall indemnify Virgin Media against losses arising from or in connection with any infringement of any Intellectual Property Rights made by a third party against Virgin Media.

11. Confidentiality.

11.1. All information of a confidential nature imparted by either party to the other party in connection with the Purchase Order, including but not limited to data of or about customers or suppliers, drawings, patterns, raw materials, designs, specifications and any information relating to the technical affairs or business or product plans of either party ("Confidential Information") shall be treated as proprietary and confidential to the party disclosing the Confidential Information.

11.2. Neither party shall use or disclose any Confidential Information of the other party without the agreement in writing of the other party except:

(a) to the extent necessary to comply with any law or regulation in which event the relevant party shall so notify the other as promptly as reasonably practicable and shall seek confidential treatment of such information;

(b) to its auditors, legal advisers and other professional advisers provided that it uses its

reasonable endeavours to procure that such persons maintain such confidentiality;

(c) in order to enforce and enjoy its rights under the Purchase Order; and

(d) to any person with a bona fide and legitimate interest in such information who enters into a confidentiality agreement including, but not limited to, a prospective purchaser of Virgin Media or its business and provided that such person only uses the information for the purpose of such bona fide and legitimate interest.

11.3. The provisions of Clause 11.2 shall not apply to:

(a) any information in the public domain otherwise than by breach of the Purchase Order;

(b) information obtained from a third party who is free to divulge the same;

(c) information that was already known to the receiving party prior to disclosure under the Purchase Order and was not previously acquired by the receiving party from the disclosing party under an obligation of confidentiality or non-use towards the disclosing party;

(d) information that can be shown by documentary evidence to have been created by one party to the contract independently from work under the Purchase Order.

12. IT Security, Virgin Media Data and Data Security, Data Protection.

Virgin Media and the Supplier shall comply with the terms and conditions of the data and security provisions set out in Annex 1 and Annex 2 to this Appendix.

13. Miscellaneous.

13.1. The Supplier will not without the prior written consent of Virgin Media in any way whatsoever advertise or publish the fact that the Supplier has entered the Purchase Order or contracted to supply to Virgin Media any Products or Services.

13.2. The Purchase Order is personal to the Supplier and the Parties shall not transfer, assign, novate, subcontract or otherwise dispose of any of their rights or obligations under the Purchase Order without the prior written consent of the other Party unless such disposal of rights/obligations is to a third party who is a “subsidiary undertaking” or “parent undertaking” (defined in sections 1161 and 1162 and schedule 7 of the Companies Act 2006) to the disposing party.

13.3. At the request of Virgin Media, the Supplier shall execute all deeds and other documents required to effect any transfer, assignment, novation, subcontracting or disposal of all or any of Virgin Media’s rights and obligations under the Purchase Order to another member of the Virgin Media group or to any purchaser of the whole or substantially all of the business undertaking of Virgin Media to which the Purchase Order relates.

13.4. Any notice required or permitted to be given by either party to the other under the Purchase Order shall be in writing addressed to that other party at its registered office or principal place of business or such other address in the United Kingdom as may at the relevant time have been notified pursuant to this provision to the party giving the notice.

13.5. The exercise or waiver, in whole or in part, of any right, remedy, or duty provided for in the Purchase Order will not constitute the waiver of any prior, concurrent or subsequent right, remedy, or duty within the Purchase Order. No single or partial exercise of any right, power, privilege or remedy under the Purchase Order shall prevent any further or other exercise thereof or the exercise of any other right, power, privilege or remedy.

13.6. If any provision of the Purchase Order is held by any court or competent authority to be illegal, void, invalid or unenforceable under the laws of any jurisdiction, the legality, validity and enforceability of the remainder of the Purchase Order in that jurisdiction shall not be affected, and the legality, validity and enforceability of the whole of the Purchase Order in any other jurisdiction shall not be affected. In these circumstances, the parties shall meet to discuss the affected provisions and shall substitute a lawful and enforceable provision which so far as possible results in the same economic effects.

13.7. The Purchase Order does not create any right or benefit enforceable by any person not a party to it (within the meaning of the Contracts (Rights of Third Parties) Act 1999).

13.8 The Purchase Order, together with any documents referred to in it, constitutes the whole agreement between the parties relating to its subject matter and supersedes and extinguishes any prior drafts, agreements, undertakings, representations, warranties and arrangements of any nature, whether in writing or oral, relating to such subject matter.

13.9 Each party acknowledges that it has not been induced to enter into the Purchase Order by any representation or warranty other than those contained in the Purchase Order and, having negotiated and freely entered into the Purchase Order, agrees that it shall have no remedy in respect of any other such representation or warranty except in the case of fraud.

13.10 The rights, powers, privileges and remedies provided in the Purchase Order are cumulative and are not exclusive of any rights, powers, privileges or remedies provided by law or otherwise.

13.11 At any time after the date hereof each of the parties shall, at the request and cost of another party, execute or procure the execution of such documents and do or procure the doing of such acts and things as the party so requiring may reasonably require for the purpose of giving to the party so requiring the full benefit of all the provisions of the Purchase Order, subject to any express restrictions in the Purchase Order on the extent of either party’s obligations under the Purchase Order.

13.12 Subject to any express provisions to the contrary each party to the Purchase Order shall pay its own costs of and incidental to the negotiation, preparation, execution and carrying into effect of the Purchase Order and in carrying out any related due diligence.

13.13 The parties acknowledge that the Supplier is an independent contractor of Virgin Media and the Supplier’s employees or employees of its agents or sub-contractors are not employees of Virgin Media. Each party is responsible for the management, direction, control, supervision, and compensation of its own employees, agents or

sub-contractors. Nothing in this Purchase Order shall be construed as creating a partnership between the parties or as authorising any party to act as agent for the other. The parties shall not pledge the credit of or make any promises on behalf of the other unless the same shall have been expressly authorised in writing by the other party.

13.14 The Supplier warrants and undertakes to Virgin Media and/or any of its affiliates that none of the personnel providing services under this Agreement are individuals to whom off-payroll working rules as issued by HMRC from time to time apply.

13.15 This Purchase Order constitutes a contract for the provision of services and not a contract of employment and to the extent that the Supplier engages contractors in the provision of the Services under this Purchase Order the Supplier confirms that it is responsible for all off-payroll workers' obligations. Accordingly the Supplier shall be fully responsible for and shall indemnify Virgin Media for and in respect of:

(a) any income tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with the performance of the Services, where the recovery is not prohibited by law. The Supplier shall further indemnify Virgin Media against all reasonable costs, expenses and any penalty, fine or interest incurred or payable by Virgin Media in connection with or in consequence of any such liability, deduction, contribution, assessment or claim other than where the latter arise out of Virgin Media's negligence or wilful default; and

(b) any liability howsoever arising from any employment-related claim or arising from any claim based on worker status (including reasonable costs and expenses) brought by the Supplier or any its employees, agents or sub-contractors against Virgin Media arising out of or in connection with the provision of the Services, except where such claim is as a result of any act or omission of Virgin Media.

13.16 Virgin Media may at its option satisfy such indemnity (in whole or in part) by way of deduction from any payments due to the Supplier.

13.17 The Supplier shall maintain all reports, records and other documents relating to performance of the Purchase Order and prices payable under the Purchase Order and shall allow Virgin Media access to all such documents at all reasonable times.

13.18 This Purchase Order and any non-contractual obligations arising from or connected with it shall be governed by English law and the Purchase Order shall be construed in accordance with English law. In relation to any legal action or proceedings arising out of or in connection with the Purchase Order (whether arising out of or in connection with contractual or non-contractual obligations), each of the parties irrevocably submits to the exclusive jurisdiction of the English courts and waives any objection to action or proceedings in such courts on the grounds of venue or on the grounds that action or proceedings have been brought in an inappropriate forum.

ANNEX 1

IT AND DATA SECURITY, DATA PROTECTION

1. IT Security.

1.1 In supplying the Services, the Supplier shall in accordance with Good Industry Practice:
- (a) take all necessary steps (and ensure that the Supplier and its subcontractor personnel take all necessary steps) to:
  - (i) ensure that no Virus is contained in or affects the Deliverables as at the date of delivery by the Supplier to Virgin Media of such items; and
  - (ii) prevent any Viruses being introduced via the Supplier Owned Systems into Virgin Media's Systems; and
- (b) use the current release of recognised market leading Virus detection software.

1.2 The Supplier shall indemnify Virgin Media for all losses incurred or suffered as a result of a breach of this Clause 1.

2. Virgin Media Data and Data Security.

2.1 The Supplier shall, in accordance with Good Industry Practice:
- (a) not use or reproduce Virgin Media's Data in whole or in part in any form except as expressly permitted by Virgin Media in accordance with this Purchase Order;
- (b) apply appropriate security procedures within the Supplier Premises and take all precautions necessary to preserve the integrity of Virgin Media's Data; and
- (c) procure that no unauthorised third party will, as a result of any act or omission of the Supplier or any of the Supplier and its subcontractor personnel, obtain access to any of Virgin Media's Data or any information forming part of or being used in connection with the Services.

2.2 The Supplier shall indemnify Virgin Media for all losses incurred or suffered by them as a result of a breach of this Clause 2.

2.3 For the avoidance of doubt, the Supplier's obligations under this Clause 2 are in addition to its obligations under Clause 3 (Data Protection) (including to the extent that any Virgin Media Data is "Personal Data" under the Data Protection Legislation).

2.4 Where there has been any breach or where the Supplier suspects there has been a breach of this Clause, the Supplier shall inform Virgin Media immediately.

3. Data Protection.

3.1 As part of the provision of Products and/or Services under this Purchase Order Virgin Media may engage the Supplier to Process Personal Data on its behalf and/or the Supplier may be able to access Personal Data and accordingly the parties agree that Virgin Media is the Data Controller and the Supplier (and each permitted subcontractor or third party engaged by the Supplier pursuant to this Purchase Order) is a Data Processor.

3.2 Neither party shall do, nor cause or permit to be done, anything which may result in a breach of the Data Protection Legislation by the other party.

3.3 The Supplier shall, at all times, comply with the Data Protection Legislation in relation to Personal Data processed by it under this Purchase Order.

3.4 Without limiting Clauses 3.2 and 3.3 the Supplier warrants, represents and undertakes to Virgin Media that:
- (a) it shall only process the Personal Data:
  - (i) on behalf of Virgin Media and in accordance with this Clause 3 and the documented instructions of Virgin Media (which may be specific instructions (including in respect of the subject matter, duration, nature, purpose, type of Personal Data, specific restrictions and categories of Data Subjects as in each case are as set out in the Purchase Order) or instructions of a general nature as set out in the Purchase Order or as otherwise notified by Virgin Media to the Supplier from time to time during the Term), and to the extent, and in such a manner, as is reasonably necessary to provide the Goods and/or Services in accordance with the Purchase Order; or
  - (ii) as required by applicable law (provided that the Supplier first informs Virgin Media of the legal requirement unless this is prohibited by such applicable law) and always in compliance with Data Protection Legislation;
- (b) it shall only (and is only authorised by Virgin Media to) engage another Data Processor to perform Processing activities in respect of Virgin Media Data on behalf of Virgin Media, or transfer or disclose any Virgin Media Data to any other party as is necessary for the provision of the Services and in such circumstances Supplier shall: (a) obtain Virgin Media's written authorisation in advance of such engagement, transfer and/or disposal; and (b) shall comply with the terms of this Purchase Order (including without limitation Clauses 3.4(c) and (d) herein). As at the date of this Agreement, Virgin Media has authorised use of those subprocessor(s) identified in the Purchase Order;
- (c) it shall: (a) enter into a written agreement ("Processor Contract") with all third parties that will Process Virgin Media Data containing obligations on such third party which are equivalent to and no less onerous than those set out in this Purchase Order (including in relation to engaging another Data Processor) and the Supplier shall promptly upon request by Virgin Media provide the relevant details of any such Processor Contract to Virgin Media; and (b) undertake a data protection impact assessment in relation to any high risk Processing activity and make available to Virgin Media in a timely manner the results of such data protection impact assessment;
- (d) it shall remain fully liable to Virgin Media for any non-compliance with the terms of this Purchase Order by any sub-contractor it appoints;
- (e) It shall not transfer any Virgin Media Data to any country or territory outside the United Kingdom, European Economic Area or to any international organisations ("International Recipient") without first obtaining the express written consent of Virgin Media and, if Virgin Media consents to the transfer of Virgin Media Data to an International Recipient, the Supplier shall ensure that such transfer (and any onward transfer): (a) is pursuant to a written contract including provisions relating to security and confidentiality of the Virgin Media Data; (b) is effected by way of a legally enforceable

mechanism for transfers of Personal Data as may be permitted under Data Protection Legislation from time to time (the form and content of which shall be subject to Virgin Media's written approval); (c) complies with Clause 3.4(a); and (d) otherwise complies with Data Protection Legislation. For the purpose of this Clause 3.4(e), Virgin Media hereby approves the use of Model Contract Clauses as a legally enforceable mechanism for transfers of Personal Data and provides a power of attorney for the Supplier to enter into any such Model Contract Clauses with an International Recipient in the name and on behalf of Virgin Media as the Data Exporter provided that Supplier shall not modify, vary, supplement or disapply any of the Model Contract Clauses or its Appendices without Virgin Media's prior written approval; and

(f) the Supplier shall maintain data secrecy in accordance with applicable Data Protection Legislation and shall take all reasonable steps to ensure that:
  (i) only those Supplier personnel and personnel of another Data Processor engaged by Supplier in accordance with this Purchase Order that need to have access to Personal Data are given access and only to the extent necessary to provide the Goods and/or Services; and
  (ii) the Supplier and any other Data Processor engaged by the Supplier are reliable, familiar with the requirements of data protection and subject to appropriate obligations of confidentiality and data secrecy in accordance with applicable Data Protection Legislation and at all times act in compliance with Data Protection Legislation and the obligations of this Clause 3;

(g) it has implemented (and shall comply with) all appropriate technical and organisational measures to ensure the security of the Personal Data, to ensure that Processing of the Personal Data is performed in compliance with the requirements of the applicable Data Protection Legislation and to ensure the protection of the Personal Data against accidental or unauthorised access, alteration, destruction, damage or loss as well as against any other unauthorised Processing. Such measures shall ensure best practice security, be compliant with Data Protection Legislation at all times and comply with the Security Measures;

(h) the Supplier shall promptly notify Virgin Media in writing: (i) if the technical and organisational measures taken by the Supplier do not fulfil the requirements of Clause 3.4(g) above; and (ii) of any advance in technology or changes in risk which mean that Virgin Media should change the Security Measures;

(i) the Supplier shall provide Virgin Media with such assistance and co-operation as Virgin Media may reasonably request to enable Virgin Media to comply with any obligations imposed on Virgin Media by Data Protection Legislation in relation to Personal Data Processed by the Supplier, including, but not limited to:

(i) on request of Virgin Media, promptly providing written information regarding the technical and organisational measures which the Supplier has implemented to safeguard Personal Data;

(ii) disclosing full and relevant details in respect of any and all government, law enforcement or other access protocols or controls which it has implemented;

(iii) notifying Virgin Media as soon as possible and as far as it is legally permitted to do so, of any access request for disclosure of data which concerns Personal Data (or any part thereof) by any governmental or other Regulator, or by a court or other authority of competent jurisdiction. For the avoidance of doubt and as far as it is legally permitted to do so, the Supplier shall not disclose or release any Personal Data in response to such request served on the Supplier without first consulting with and obtaining the written consent of Virgin Media; and

(iv) notifying Virgin Media as soon as possible of any legal or factual circumstances preventing the Supplier from executing any of the instructions of Virgin Media.

3.5 The Supplier shall inform Virgin Media immediately of any enquiry, complaint, notice or other communication in connection with the Goods and/or Services or Virgin Media's compliance with Data Protection Legislation from any Regulator or any individual, which the Supplier or any third party appointed by the Supplier receives. The Supplier shall provide all necessary assistance to Virgin Media to enable Virgin Media to respond to such enquiries, complaints, notices or other communications and to comply with Data Protection Legislation. For the avoidance of doubt, the Supplier shall not respond to any such enquiry, complaint, notice or other communication without the prior written consent of Virgin Media. To the extent that Supplier is legally required to provide to any third party information in relation to Virgin Media Data on the basis of mandatory statutory provisions, the Supplier shall inform Virgin Media, in writing and in due time prior to providing the information, of the recipient, the date and time, the content of the information to be issued, and the legal basis thereof.

3.6 The Supplier shall notify Virgin Media immediately in writing if it becomes aware of any Data Breach and provide Virgin Media, as soon as possible, with complete information relating to a Data Breach, including, without limitation, the nature of the Data Breach, the nature of the Personal Data affected, the categories and number of Data Subjects concerned, the number of personal data records concerned, measures taken to address the Data Breach, the possible consequences and adverse effect of the Data Breach and any other information Virgin Media is required to report to the relevant Regulator or Data Subject. The Supplier shall maintain a log of Data Breaches including facts, effects and remedial action taken. The Supplier, at its own cost, shall take all steps to restore, re-constitute and/or reconstruct any Personal Data which is lost, damaged, destroyed, altered or corrupted as a result of a Data Breach, with all possible speed and as if they were the Supplier's own data, and shall provide Virgin Media with all reasonable assistance in respect of any such Data Breach. The Supplier shall also provide all

reasonable assistance to Virgin Media in relation to Virgin Media's compliance with the Data Protection Legislation.

3.7 Where Virgin Media is legally required to provide information regarding the Personal Data and its Processing to any Data Subject or any third party, the Supplier shall support Virgin Media in the provision of such information as instructed by Virgin Media.

3.8 The Supplier shall implement appropriate technical and organisational measures to provide Virgin Media with co-operation and assistance in complying with any Data Subject rights under the Data Protection Legislation (including access requests, right to be forgotten and data portability) received by, or on behalf of, or in connection with Virgin Media or this Purchase Order.

3.9 The Supplier shall support and assist Virgin Media in fulfilling its legal requirements with regards the creating and updating a Process register and undertaking required risk assessments for the Processed personal data, especially but not limited to changes in the technical and organizational measures. The Supplier shall maintain complete, accurate and up to date written records of all categories of Processing activities carried out on behalf of Virgin Media containing such information as required under Data Protection Legislation and any other information Virgin Media reasonably requires ("Processing Records"), and shall make the Processing Records available to Virgin Media on request in a timely manner, where reasonably required by Virgin Media to demonstrate compliance by Virgin Media with its obligations under Data Protection Legislation and this Purchase Order, which Virgin Media may disclose to any relevant Regulator.

3.10 The Supplier shall permit Virgin Media, or a third-party auditor acting under Virgin Media's direction, to conduct, at Virgin Media's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to the Processing of Personal Data, and its compliance with this Purchase Order and Data Protection Legislation. Virgin Media may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with these procedures and with Data Protection Legislation (which may include, by way of example and without limitation, any assessment of any qualified independent third party engaged by the Supplier) in lieu of or in addition to conducting such an audit, assessment or inspection.

3.11 The Supplier shall notify Virgin Media prior to adopting a new or updated type of Processing (including, without limitation, the use of new technology to continue current Processing) in respect of Personal Data and at Virgin Media's request the Supplier shall participate in a data protection impact assessment in respect of the new or updated type of Processing which is being proposed (and provide assistance to Virgin Media in consulting with the relevant Regulator in relation to high risk Processing), as required from time to time by Virgin Media.

3.12 After the termination of the Processing of the Personal Data or earlier upon request of Virgin Media, the Supplier shall cease all use of Personal Data and, at Virgin Media's election, irrevocably delete, destroy, or transfer (in a mutually agreed format and by a mutually agreed method) to Virgin Media (or a third party nominated by Virgin Media) all Personal Data and copies thereof in its possession as well as any Processing products produced with such Personal Data. The deletion and/or destruction thereof are to be documented in a suitable manner and evidenced to Virgin Media.

3.13 The Supplier shall confirm that it (i) has appointed an in-house data protection officer if required by applicable Laws; and (ii) shall be obligated to maintain the appointment of an in-house data protection officer for the duration of the term of this Purchase Order. The Supplier shall provide the name of such data protection officer to Virgin Media in writing and shall advise Virgin Media without undue delay of any change in such officer.

3.14 The Supplier shall indemnify Virgin Media and keep Virgin Media fully and effectively indemnified against all costs, claims, demands, fines, awards, expenses (including legal costs and disbursements on a full indemnity basis), losses (including direct and indirect losses and loss of profits), actions, proceedings and liabilities of whatsoever nature arising from or incurred by Virgin Media or its affiliates in connection with any failure of the Supplier or any third party appointed by the Supplier to comply with the provisions of this Purchase Order and/or Data Protection Legislation in respect of its Processing of Virgin Media Data or acting outside Virgin Media's lawful Processing instructions.

3.15 The Supplier shall not acquire any rights (including any retention rights) in the Personal Data Processed under this Purchase Order.

3.16 For the purpose of this Clause 3 (Data Protection), the following words and phrases shall have the following meaning unless the context otherwise requires:

"Data Breach" means any unauthorised or unlawful Processing, disclosure of, or access to, Personal Data or any accidental or unlawful destruction of, loss of, alteration to, or corruption of Personal Data;

"Data Controller" has the meaning set out in the Data Protection Legislation;

"Data Exporter" has the meaning set out in the Model Contract Clauses;

"Data Processor" has the meaning set out in the Data Protection Legislation;

"Data Protection Legislation" means the GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003, any applicable laws in respect of data privacy and/or the processing of Personal Data including any laws made under them, any laws which implement them and any amendment or re-enactment of any of them, and including where applicable, the guidance and codes of practice issued by Regulators;

"Data Subject" has the meaning set out in the Data Protection Legislation;

"GDPR" means the General Data Protection Regulation (EU) 2016/679 as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2020 (including as further amended or modified by the laws of the United Kingdom or a part of the United Kingdom from time to time);

“Good Industry Practice” means, in relation to any undertaking and any circumstances, the exercise of the skill, care, prudence, efficiency, foresight and timeliness which would be expected from a highly skilled, trained and experienced person under the same or similar circumstances;

“Model Contract Clauses” means the standard contractual clauses set forth in the European Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC or the standard contractual clauses as amended or modified by the laws of the United Kingdom;

“Personal Data” has the meaning set out in the Data Protection Legislation;

“Processing” has the meaning set out in the Data Protection Legislation (and “Process” and “Processed” shall be construed accordingly);

“Processing Records” has the meaning given in Clause 17.9;

“Regulators” means those government departments and regulatory, statutory and other bodies, entities and committees which, whether under statute, rule, regulation, code of practice or otherwise, are entitled to regulate, investigate or influence the matters dealt with in this Purchase Order (and “Regulator” shall be construed accordingly);

“Security Measures” means Virgin Media’s security policies and measures (including IT policies and measures) for the protection of Personal Data issued to Supplier by Virgin Media from time to time which as at the date hereof are as specified in Annex 2; and

“Virgin Media Data” means all Personal Data, in whatever form or medium which is: (i) supplied, or in respect of which access is granted to the Supplier (or any approved third party) whether by Virgin Media or otherwise in connection with this Purchase Order, or (ii) produced or generated by or on behalf of the Supplier (or any approved third party) in connection with this Purchase Order.

ANNEX 2

SECURITY MEASURES

Security Procedures. Supplier will implement and maintain reasonable and appropriate measures designed to secure Virgin Media's Confidential Information against accidental or unlawful loss, access or disclosure in its collection, receipt, transmission, storage, disposal, use and disclosure of such Confidential Information.

Supplier will properly configure the Services and take steps to maintain security, protection and backup of Virgin Media's Confidential Information and data ("Data") which may include routine archiving of Data and the use of encryption technology to protect Data from unauthorized access.

Without limiting the generality of the preceding sentence, Supplier shall have in place, at a minimum physical, technical, administrative, and organizational measures and safeguards that provide for and ensure:

(i) protection of business facilities, paper files, servers, computing equipment, and backup systems containing Data;
(ii) network, application (including databases) and platform security;
(iii) business systems designed to optimize security and proper disposal of Data in accordance with the terms of this Agreement;
(iv) secure transmission and storage of Data using strong cryptography in accordance with industry best practices;
(v) mail exchange protected with TLS and set DMARC policy, preferably DKIM signed;
(vi) authentication and access control mechanisms over Data, media, applications, operating systems, and equipment;
(vii) personnel security and integrity, including background checks where consistent with applicable law;
(viii) training to Personnel on how to comply with Supplier's physical, organizational, technical, and administrative information security safeguards and confidentiality obligations under this Agreement;
(ix) storage limitations such that Data resides only on servers located in EU data centers that comply with industry standard data center security controls, and restrictions to ensure that Supplier personnel do not place any Data files on any notebook hard drive or removable media, such as compact disc or flash drives, unless encrypted;
(x) developing, implementing, updating and keeping current industry standard
    (a) backup systems (emergency and otherwise), network technology, firewalls, intrusion-detection and prevention systems, anti-virus protection and other network and technological security systems, and
    (b) computer systems, networks, and other equipment and software that secure data (including the Data) during storage, manipulation, and dissemination and processes that secure data (including the Data) during system or network changes;
(xi) routinely reviewing and updating network technology, anti-virus programs, backup systems, and other technological security systems;
(xii) regular testing for common coding weaknesses and vulnerabilities prior to deployment and during upgrades; and
(xiii) vulnerability management such that vulnerabilities are assessed and addressed in accordance with industry best practice.

Access Limitations. Supplier will restrict access to Data only to those Supplier personnel ("Personnel") who have a need to know or otherwise access the Data to enable Supplier to perform its obligations under this Agreement, provided that:

(i) a background check has been conducted of those Personnel; and
(ii) those Personnel are bound in writing by obligations of confidentiality sufficient to protect the Data in accordance with the terms of this Agreement.

Supplier shall be responsible at all times for the compliance of all Personnel with Supplier's obligations under this Agreement.

***Breach Notification Procedures*.**

(i) Virgin Media may contact Supplier Technical Support for assistance in resolving obligations associated with a data security breach or incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so (hereinafter a "Security Breach");

(ii) Supplier shall notify Virgin Media of a Security Breach no later than twenty-four (24) hours after Supplier becomes aware of it.

(iii) Immediately following Supplier's notification to Virgin Media of a Security Breach, the parties shall coordinate with each other to investigate the Security Breach. Supplier agrees to cooperate with Virgin Media in its handling of the matter, including, without limitation obtaining and making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise reasonably required by Virgin Media.

Right to Audit. Virgin Media shall have the right to audit Supplier to ensure compliance with this Schedule in accordance with the terms of this agreement.

Personal Information. Where the Supplier is processing personal information, technical and organizational security measures shall be implemented by the Supplier:

The Supplier shall implement the following additional measures described in this Schedule, provided that the measures directly or indirectly contribute or can contribute to the protection of personal data under the agreement concluded between the Parties for the processing of data. If the Supplier believes that a measure is not necessary for the respective order, they are to justify this and come to an agreement with the Virgin Media on an individual case basis.

The technical and organizational measures are subject to technical progress and development. In this respect the Supplier is permitted to implement alternative

adequate measures. The level of security must align with industry security best practice and not less than the measures set forth herein. Major changes must be agreed with Virgin Media and documented. The Supplier must provide proof in cases of doubt that the alternative measure provides the same protection objective and a comparable level of protection.

Virgin Media may at any time demand changes to the technical and operational measures described under this schedule, if, in the sole discretion of Virgin Media, Virgin Media deems such change to be necessary to fulfill legal requirements with regards to data protection and security matters in conjunction to the Services provided under the Service Agreement by the Supplier. Virgin Media also reserves the rights to audit the supplier against these controls.

1. Physical Access control

Unauthorised persons are to be denied access to data processing equipment, with which personal data is processed or used.

The Supplier shall take the following physical access control measures, insofar as personal data is processed in the premises/buildings of the Supplier. Access to such data outside of these premises/buildings is not permitted:

1. Restriction of access rights to office buildings, data centres and server rooms to the minimum necessary.
2. Effective control of access rights through an adequate locking system (for example, security key with documented key management, electronic locking systems with documented management of authorization).
3. A Comprehensive and fully documented processes must be in place for attainment, change and withdrawal of access authorization.
4. Regular and documented review of access authorizations granted to date.
5. Reasonable measures for the prevention and detection of unauthorized access and access attempts (e.g. regular review of burglary protection of the doors, gates and windows, alarm systems, video surveillance, security guards, security patrol).
6. Written regulations for employees and visitors for dealing with technical access security measures.

2. Logical Access Control to systems

Use by unauthorized persons of data processing systems must be prevented.

The Supplier shall take the following measures to control access to systems and networks in which order data is processed or via which admission to order data is possible:

1. Restriction of admission rights to IT systems and non-public networks to the minimum necessary.
2. Effective control of Authentication, Authorization and Accounting through personalized and unique user identifications and secure authentication process.
3. When using passwords for authentication regulation shall be adopted to ensure the quality of passwords in terms of length, complexity and change frequency. Technical testing methods shall be implemented in order to ensure password quality.
4. When using asymmetric key methods (e.g. certificates, private-public-key-methods) for authentication, it shall be ensured that secret (private) keys are always protected with a password (passphrase). The requirements in accordance with above paragraph 3 are to be observed.
5. Full reviews of all accounts must be regularly undertaken and access removed if not required on a regular basis
6. Regular and documented review of the logical access authorizations granted to date
7. Appropriate measures to secure the network infrastructure must be undertaken (e.g. network port security IEEE 802.1X, Intrusion Detection Systems, use of 2-factor authentication for remote access, separation of networks, content filtering, encrypted network protocols, etc.)
8. Written regulations for employees when dealing with the above security measures and safe use of passwords.
9. Ensuring the immediate installation of critical/ or important security-updates/patches
    a. in Controller operating systems,
    b. in server operating systems, which are accessible via public networks (e.g. web server),
    c. in application programs (including browser, plugins, PDF reader, etc.) and
    d. in security infrastructure (virus scanners, firewalls, IDS systems, content filters, routers, etc.) within 48 hours after publication by the manufacturer as well as
    e. in server operating systems of internal server within 1 week after publication by the manufacturer

3. Access control to data

It shall be ensured that persons authorized to use a data processing system can have access exclusively to the data, subject to their access authorization, and that personal data cannot be read, copied, changed or removed without authorization during processing, use and after storage.

The Supplier shall take the following measures for access control, insofar as they themselves are responsible for the access authorization to order data:

1. Restriction of access authorization to data to the bare minimum required.
2. Effective control of access authorization through an adequate rights and role concept.
3. A Comprehensive and fully documented process for authorizing access, changing,

copying and withdrawal of data must be in place

4. Regular and documented reviews of the assigned access authorizations to date
5. Reasonable measures for the protection of terminal equipment, servers and other infrastructure elements against unauthorized access (e.g. multi-level virus protection concept, content filtering, application firewall, intrusion detection systems, desktop firewalls, system hardening, content encryption) must be undertaken
6. Data media encryption - aligned to the current state of the art technology - algorithms to be enforced for the protection of mobile devices (laptops, tablet PCs, smartphones, etc.) and data media (external hard drives, USB sticks, memory cards, etc.)
7. Logging of accesses, to data by all users including administrators.
8. Technical security measures for export and import interfaces (hardware and application related).

The Supplier shall have the following obligations to cooperate with the access control, <u>unless</u> they are managing the access authorization to order data:

1. A Comprehensive and fully documented process for application, change and withdrawal of access authorizations in their area of responsibility
2. Regular and documented review of the assigned access authorizations to date as far as is possible
3. Immediate notification to the Controller if the existing access authorizations are no longer required.

4. Transmission control

The Supplier shall provide the data to be processed in a transmission procedure to be defined in a contract/order. The results of the processing will also be transmitted back to the Controller in a defined transmission procedure. The method of transmission as well as the security measures of the transmission (transmission control) is to be set according to requirements; in particular the use of state of the art encryption technology is to be provided for.

It shall be guaranteed that personal data is not read, copied, changed or removed without authorization during electronic transfer or during transportation or storage on data carriers, and that it can be checked and established at which locations a transfer of personal data by means of equipment for data transmission is provided for.

The Supplier shall take the following measures for transmission control, insofar as order data are received, transferred or transported by the Supplier:

1. Appropriate measures to secure the network infrastructure (e.g. network port security IEEE 802.1X, Intrusion Detection Systems, use of 2-factor authentication for remote access, separation of networks, content filtering, encrypted network protocols, etc.) must be applied.
2. Data media encryption with - according to the current state of the art technology - algorithms to be classified as safe for protection of mobile devices (laptops, tablet PCs, smartphones, etc.) and data media (external hard drives, USB sticks, memory cards, etc.)
3. Use of encrypted communication protocols (such as TLS-based protocols).
4. Inspection mechanisms to identify remote terminals during transmissions.
5. Checksums adjustment with received data
6. Written regulations for employees for the handling and security of mobile devices and data carriers.

5. Data Entry control

It shall be ensured that it can be subsequently checked and verified whether and by whom personal data can be entered into, modified in or removed from data processing systems.

The Supplier shall take the following measures to control entry onto its systems that serve the processing of data or enable or provide access to such systems:

1. Creation and revision-secure storage of process protocols.
2. Securing of backup log files against tampering
3. Logging and analysis of failed login attempts
4. Ensuring that no group accounts (also administrators or root) can be used

6. Data Processing control

It is necessary to ensure that any personal data that is processed can only be processed in accordance with the instructions of the Controller.

The Supplier shall take the following measures for Data Processing control:

Processes and documentation for

1. the selection of (sub)processors under data protection law and technical aspects
2. ensuring prescribed statutory preliminary inspection of (sub)processors in accordance applicable law provisions
3. ensuring the timely instruction of operational data protection officers upon introduction of new or changes to existing procedures for processing personal data
4. obligations of all persons responsible for processing of personal data to maintain data secrecy pursuant to applicable law provisions
5. regular verification of the correctness of the application of data processing programs by which personal data is processed
6. ensuring the familiarization of the persons entrusted with data processing subject with the relevant data protection and Controller-specific regulations

7. maintenance of the qualification of the operational data protection officer (if appointed)
8. ensuring the prompt notification of the Controller in the event of an unlawful acquisition of knowledge of personal information or otherwise protected information
9. ensuring the immediate correction, blocking and deletion of order data upon instruction by the Controller

7. Availability control

It shall be ensured that personal data are protected against accidental destruction or loss.

The Supplier shall implement the following measures to control availability, provided that the processing is required in order to maintain productive services:

1. Operation and regular maintenance of fire alarm systems in server rooms, data centres and critical infrastructure spaces.
2. Creating daily backups
3. Ensuring backup storage in a separate fire compartment
4. Regular review and testing of backup integrity
5. Processes and documentation for the recovery of systems and data

8. Appropriation control

It shall be ensured that data collected for different purposes can be processed separately.

The Supplier shall take the following measures for the separation of order data, provided that they lie in their area of responsibility:

1. Logical and/or physical separation of test, development and production systems
2. Controller separation within the processing systems and at interfaces
3. Ensuring continued identifiability of the order data

9. Retention and Deletion of data

Personal data shall be retained only for as long as required and deleted when the processing fulfilment is complete. **The Supplier shall take the following measures to ensure the deletion of data, provided that they lie within their area of responsibility:**

1. Ensure continued erasability of data upon request of the Controller
2. Processes, tools and documentation for secure deletion in such a way that recovery of the data is not possible using current state of the art technology
3. Guidelines for employees on how and when which data should be deleted.