GLOBAL INSTALLATION AND SERVICE STANDARD TERMS

1 BASIS OF CONTRACT

1.1 From time to time, Inmarsat may request Contractor (each a "Party") on a non- exclusive basis to perform installation and related services ("Services") for Inmarsat as set out in a purchase order for the supply of Services (the "Work Order"). The Work Order constitutes an offer by Inmarsat to purchase Services from Contractor in accordance with these terms and conditions ("Terms") and as specified in the Statement of Work contained in exhibits 2 to 5 of the Work Order (the "SOW").

1.2 The Work Order shall be deemed to be accepted upon Contractor signing and returning a copy of the Work Order, at which point this Agreement shall come into existence ("Effective Date"). For the purpose of these Terms, "Agreement" shall mean the agreement between Inmarsat and the Supplier for the supply of Services in accordance with these Terms and the accompanying Work Order(s).

1.3 The Agreement shall continue from the Effective Date until terminated by Inmarsat or Contractor upon sixty (60) calendar days prior written notice or as otherwise provided herein.

2 SCOPE OF SERVICES

2.1 Contractor agrees to perform the Services in a professional manner and in accordance with the provisions of this Agreement.

2.2 Notwithstanding the foregoing, Inmarsat is under no obligation to request Contractor to perform Services, and Contractor is under no obligation to accept a request for Services from Inmarsat.

2.3 Other services, and rates, may be added from time to time and Inmarsat reserves the right, at its option, to request that additional Work Orders for any additional products or services be added to this Agreement, pursuant to the mutual agreement of the parties. In the event that a Work Order is initiated or revised orally, Inmarsat will issue a follow-up Work Order (or amended Work Order as appropriate) to the Contractor for execution in accordance with the terms and conditions of this Agreement.

2.4 Contractor shall be solely responsible for Contractor's personnel observing Inmarsat's or Inmarsat's customer's site rules and regulations, including but not

limited to: security requirements, use of safety equipment and safety procedures, proper grooming, appropriate dress, and working in harmony with all others while present at such site. Inmarsat shall have the right for any reason to request that Contractor discontinue furnishing any person provided by Contractor hereunder. Said discontinuance shall take effect immediately upon Inmarsat's written or oral notice to Contractor. In the event Contractor is required to remove personnel pursuant to this Article, Contractor will not be relieved of its obligation to perform hereunder.

2.5 The Contractor shall comply with Inmarsat's 'Supplier Relationship Security Schedule', which is set out in Annex 1 of this document. From time to time, Inmarsat may update this Schedule to the Contractor. For avoidance of doubt, 'Supplier' as referred to in the Supplier Relationship Security Schedule will mean 'Contractor'.

3 INVOICES AND PAYMENTS

3.1 Upon receipt of an invoice, Inmarsat will remit payment to Contractor within sixty (60) calendar days.

3.2 Inmarsat shall have no obligation to pay Contractor for any other charges unless such charges are expressly authorised in a Work Order and this Agreement. In the event that any work is required to be performed to complete an installation which is beyond that specified in the SOW, Contractor must seek the prior approval of the applicable end user and Inmarsat to perform such work.

3.3 Contractor shall maintain accurate records to verify and support any invoices (electronic or otherwise) generated in the event of any disputes. Contractor's satisfactory performance and invoicing for Services hereunder will be in accordance with generally accepted accounting principles and practices uniformly and consistently applied in a format that will permit review. Additionally, and notwithstanding Article 16, Inmarsat will be entitled to provide a copy of any information obtained pursuant to this Article 3.3, to Inmarsat's customer to whom such information relates.

3.4 In the case of business travel, Inmarsat will only reimburse technician for economy class travel using a commercial carrier (to include airplane, train, bus, etc.).

4 TAXES

4.1 Except as expressly provided in this Article 4 (Taxes), the rates and charges set forth in the Work Order include all taxes of whatever nature levied or assessed against this Agreement, the Work Orders and Services hereunder or any transaction related thereto.

4.2 Contractor hereto agrees to pay, and to hold Inmarsat harmless against, any penalty, interest, additional tax or other charge that may be levied or assessed as a result ofthe delay or failure of the Contractor for any reason to pay any tax or file any return or information required by law, rule or regulation or by this Agreement to be paid orfiled by Contractor.

5 TERMINATION

5.1 Termination/ Rescheduling of Work Orders

5.1.1 Subject to Article 5.3 below, Inmarsat may terminate or reschedule any Work Order immediately by written notice to Contractor, for any reason or for no reason, and without penalty or liability. Such notice shall specify the effective date of termination or the reschedule date.

5.1.2 Notwithstanding the foregoing, if Inmarsat terminates or reschedules a Work Orderwhile Contractor is performing such Work Order, Inmarsat will be liable to pay to Contractor all costs reasonably and actually incurred by Contractor in relation to the terminated Work Order. Inmarsat will only be liable to pay such reasonable costs incurred up to the time that such Work Order is terminated by Inmarsat. Theforegoing is Contractor's sole remedy in the event that Inmarsat terminates or reschedules a Work Order, whilst Contractor is performing such Work Order.

5.1.3 In case Inmarsat has ordered hardware with Contractor, Inmarsat will be obliged to purchase the hardware when Contractor has ordered it with their supplier. In such cases Contractor is obliged to deliver these goods to Inmarsat.

5.2 Default

If Contractor is in default of its obligations under this Agreement or any Work Order hereunder and such default is not promptly remedied by Contractor after written notice thereof by Inmarsat, Inmarsat may, in addition to all other rights and remedies provided by law or this Agreement, terminate this Agreement and/or anyWork Order which may be affected by such default.

5.3 Consequences of Termination or Cancellation

5.3.1 In the event that Inmarsat terminates this Agreement or any Work Order hereunder pursuant to any provision of this Agreement, in no event will Inmarsat be liable for any indirect, special, incidental, reliance or consequential damages resulting from such termination, including without limitation, loss of business profits.

5.3.2 In the event that any Work Order is terminated for any reason other than breach by Contractor, Contractor shall immediately cease performing Services covered by such Work Order. In such event, the provisions of Article 5.1 shall apply.

5.3.3 In the event that Inmarsat terminates this Agreement pursuant to Articles 5.2 (Default) or 7.2 (Breach of Warranty) herein, Inmarsat may, at its option, and in addition to any other remedies available to it, obtain comparable services from third parties, and Contractor will reimburse Inmarsat for any additional costs and expenses which may be occasioned to Inmarsat thereby with such reimbursement limited to the value of the initial Work Order.

5.3.4 Within ten (10) calendar days of termination, cancellation or other expiration of this Agreement, Contractor shall return to Inmarsat all papers, written materials, properties, other materials and other information furnished to Contractor by Inmarsat under this Agreement. Each Party shall provide the other such reasonable assistance as may be necessary for an orderly, non-disruptive transition subsequent to termination.

5.3.5 The terms, conditions and warranties contained in this Agreement that are intended to survive the performance hereof by either or both Parties hereunder shall so survive the completion of performance, cancellation or termination of this Agreement or any Work Order hereunder.

6. EXCUSABLE DELAYS

Neither Party to this Agreement shall be liable for its failure to perform any of its obligations hereunder during any time period in which its, or its subcontractors' or vendors', performance is delayed by fire, flood, extreme weather conditions precluding performance, lack of availability of equipment from Inmarsat, war, embargo, strike or riot, or the intervention of any government authority ("Excusable Delay"), provided the cause of such Excusable Delay is beyond the reasonable control and without the fault or negligence of the non-performing Party, its subcontractors or vendors and further providing that the Party suffering such Excusable Delay immediately notifies the other Party of the delay. In the event of an Excusable Delay the delivery requirements for such performance shall be extended by a mutually agreed upon term in writing. Notwithstanding the above, Inmarsat may at its option, without liability other than to reimburse Contractor for actually incurred reasonable costs and expenses to the date of termination, terminate any Work Order that is delayed more than ten (10) calendar days because of any Excusable Delay.

7. WARRANTIES

7.1 Contractor hereby warrants and represents that all Services provided hereunder shall be performed by qualified personnel promptly and with diligence, in strict accordance with the descriptions of such Services in these Terms, the SOW, or in any Work Order and to Inmarsat's satisfaction. For a period of twelve (12) monthsfrom the applicable installation date Contractor shall remedy, repair or reinstall, asnecessary and at no additional charge to Inmarsat, any Services provided under this Agreement which are found to be defective and in breach of the above warranty for said period. Further, for a period of twelve (12) months from the applicable installation date Contractor shall remedy, repair or reinstall, as necessaryand at no additional charge to Inmarsat, any material provided under this Agreement which is found to be defective and in breach of the above warranty forsaid period.

7.2 If during the twelve (12) months after the completion of the installation performed by Contractor for Inmarsat, Inmarsat determines that there is a problem which constitutes a breach of warranty, Inmarsat will notify Contractor and Contractor shall promptly investigate such breach and advise Inmarsat of Contractor's planned corrective action after which Contractor shall promptly re-perform by providing other personnel or take such other action as may be required to correct such breach of warranty at no additional charge to Inmarsat. If such breach of warranty causesInmarsat's customer's system to be affected or has/may cause some form of structural damage to Inmarsat's customer's premises, then Contractor will remedy such breach of warranty to Inmarsat's reasonable satisfaction within four (4) calendar days from Inmarsat's notice to Contractor. If such breach of warranty is not causing Inmarsat's customer's system to be affected, and does not pose any threat to the structural integrity of Inmarsat's customer's premises, then Contractor will remedy such breach of warranty to Inmarsat's reasonable satisfaction within ten (10) business days from Inmarsat's notice to Contractor.

7.3 Contractor will deliver the work as stated in the SOW and any approved additional work by performing acceptance tests in the presence of Inmarsat's customer's representative. Inmarsat's customer shall have discretion as to accept the Work Order upon completion. Upon acceptance of the Work Order, the warranty set forth in Article 7.2 above shall apply. All defects shall be remedied in accordance with the terms set forth herein. Notwithstanding the foregoing, Contractor shall not be held liable pursuant to Articles 7.2 and 7.3 for unauthorised modification, tampering, or negligence of Inmarsat or its customer.

8. INFRINGEMENT INDEMNITY

Contractor represents that the use of any and all tools and materials furnished by Contractor and used in the performance of the Services does not infringe a patent,

copyright, or federal, state or common law service mark, trademark or any other proprietary rights of a third party. Contractor will protect, defend and indemnify and hold Inmarsat harmless from and against any and all claims, demands, causesof action, loss, damage, expense or liability of every type and character (individually and collectively "Claims") that may result by reason of any such infringement, provided further that Inmarsat provides prompt written notice to Contractor ofany Claim.

9. NON-COMPETE RESTRICTION

CONTRACTOR AGREES NOT TO SOLICIT WORK RELATING TO THE INSTALLATION OR MAINTENANCE OF SATELLITE EQUIPMENT OR TAKE ORDERS RELATING THERETO DIRECTLY FROM INMARSAT'S CUSTOMERS WHO HAVE BEEN INTRODUCED BY INMARSAT TO CONTRACTOR FOR INSTALLATION, MAINTENANCE AND/OR RELATED WORK THAT IS SUBSTANTIALLY RELATED TO
THE SOW. IN ACCORDANCE WITH THE FOREGOING, if an Inmarsat Customer contacts the Contractor directly or indirectly to request equipment or service, the Contractor will refer the Customer to Inmarsat and notify Inmarsat immediately. The Contractor agrees this Article 9 is binding upon the Contractor during the Term of this Agreement, as described in Article 1 of these Terms, and for one (1) year after termination of this Agreement.

10. INDEPENDENT CONTRACTOR

Contractor hereby declares and agrees that Contractor is engaged in an independent business and will perform its obligations under this Agreement as independent contractor and not as the agent or employee of Inmarsat; that the persons performing Services hereunder are agents, employees or subcontractors of Contractor and are not employees or agents of Inmarsat; that Contractor hereby retains the right to exercise full control of and supervision over the performance ofContractor's obligations hereunder and full control over the employment, direction, compensation and discharge of all employees assisting in the performance of suchobligations; that Contractor will be solely responsible for all matters relating to payment of such employees, including compliance with workers' compensation, unemployment, disability insurance, social security, withholding and all other federal, state and local laws, rules and regulations governing such matters; and that Contractor will be responsible for Contractor's own acts and those of Contractors agents and employees during the performance of Contractors obligations under this Agreement. In addition, Contractor agrees that it will require its agents to obtain all necessary licenses and business licenses required to perform the Services hereunder.

11. WORK PRODUCT

Contractor shall install, maintain or service the products as described in the SOW or Work Order issued by Inmarsat and accepted by Contractor.

12. INDEMNIFICATION

12.1 Contractor shall hold harmless and indemnify Inmarsat and its affiliated companies (including its parent company), officers, directors, employees, representatives, insurers, consultants, and customers, and agents of all of the foregoing, from anyloss, cost, damage, claim, expense or liability, including, but not limited to, liability as a result of injury to or death of any person or damage to or destruction or lossof any property arising out of, or as a result of or in connection with the performance of this Agreement and/or the Services and directly or indirectly caused, by the acts or omissions, negligent or otherwise, of Contractor or a subcontractor or an agent of Contractor or an employee of any one of them, be itactive or passive, except where such loss, cost, damage, claim, expense or liability arises solely from the negligence of Inmarsat, its officers, directors and other employees and agents. As used in the preceding sentence, the words "any person" shall include, but shall not be limited to, a contractor or an agent of Contractor or Inmarsat, and an employee of Inmarsat, Contractor or any such contractor or agent; and the words "any property" shall include, but shall not be limited to, property of Inmarsat, Inmarsat's customers, Contractor or any such contractor or agent or of an employee of any of them. Upon request of Inmarsat, Contractor shall, at no cost or expense to Inmarsat, defend suits asserting a claim for loss, damage or liability specified above, and Contractor shall pay costs and attorneys' fees that may be incurred by Inmarsat in connection with any such claims or suits or in enforcing the indemnity granted above.

12.2 Contractor shall also indemnify and hold Inmarsat harmless from and against, any direct damage, liability or expense (including reasonable attorney's fees and other expenses of investigating or defending claims) any claims made by a third party, including but not limited to any third-party dealer or installation company, which may enter into subcontracts or other arrangements with Contractor to fulfil any ofobligations set forth herein, which (a) arise directly as a result of Contractor's responsibilities hereunder, or (b) result from Contractor's having made any warranty or representation to any such third party, or (c) any act or omission of Contractor with respect to such third party.

13. LIMITATION OF LIABILITY

Except for the indemnity provisions set forth above, neither Party shall be liable tothe other for any indirect, consequential, special, reliance or incidental damages, including without limitation loss of business profits, arising out of or in connection

with the performance or non-performance of any obligations under this Agreement whether or not due to any negligent act or omission on the part of the applicable Party or its subcontractors, for whatever reason, and whether or not they have been advised of the possibility thereof.

14. INSURANCE

Without in any way limiting the obligations set forth in Article 12 (Indemnification) above, Contractor shall maintain in full force and effect insurance minimums of **$1million (USD)** of general liability insurance. The insurance required above shall remain in full force and effect as long as either Contractor or Inmarsat may have any potential liability pursuant to this Agreement.

15. LIENS

If at any time or times before or after the work specified in a Work Order issued hereunder is completed, any lien or notice of lien shall be recorded or stop work notice against Contractor or its subcontractors shall be served upon Inmarsat or Inmarsat's customers, for labour performed upon, or for furnished materials for use in, or for furnishing appliances, teams or power contributing to, said work, Contractor shall promptly procure the discharge of any or all such liens and claims in a manner satisfactory to Inmarsat. If Contractor shall not have settled same within a reasonable period of time, not to exceed thirty (30) calendar days after Contractor has received notice, either actual or constructive, of the existence of such a lien, Inmarsat shall have the right to procure the discharge of such liens, and in such event Contractor shall reimburse Inmarsat for all monies that the latter may be compelled to pay in procuring the discharge thereof including costs and reasonable attorneys' fees; and Inmarsat shall have the right to satisfy said obligation, to the extent possible, by deduction from future payments due Contractor under such Work Order, this Agreement or otherwise.

16. CONFIDENTIAL INFORMATION

16.1 The Parties acknowledge that in the course of their performance of this Agreement each Party will come into the possession of confidential information of the other Party ("Disclosing Party"). For the purposes of this Agreement "Confidential Information" means any and all information of a commercial, technical or financial nature relating to a Party, which is not generally available to the public and which is disclosed by one Party to the other for the purposes of this Agreement. This includes, without limitation, data, know-how, secret formulae, processes, designs, photographs, drawings, specifications, patentable information and software programs, regardless of form, format or media and whether communicated or obtained through meetings, documents, correspondence or inspection of a tangible

item that is in each case either i) by its very nature confidential; ii) is marked as such; or iii) it is reasonable to assume to be confidential from the context.

16.2 Confidential Information shall remain the sole and exclusive property of the Disclosing Party and may not be disclosed or used by the other Party ("Receiving Party") without the Disclosing Party's prior written consent for any purpose other than the discharge of its obligations under this Agreement. No further use of the Confidential Information will be made after the termination of this Agreement.

16.3 Confidential Information shall not include information or parts thereof for which the Receiving Party can furnish demonstrable evidence that:

16.3.1 it was known or generally accessible before the date of its receipt from the Disclosing Party; or

16.3.2 it became known or generally accessible after the date of its receipt from the Disclosing Party without the Receiving Party being responsible; or

16.3.3 was made accessible to the Receiving Party at any time by an authorised third party not in breach of any obligation of confidentiality with respect to such information.

16.4 Each Party will make available the other Party's Confidential Information only to its officers, representatives and employees and on a need to know basis and all persons to whom the Confidential Information is made available shall be made aware of the strictly confidential nature of the Confidential Information and the restrictions imposed hereunder on the use thereof and further, have agreed to abide by the specific obligations imposed under this clause 16. Both Parties shall ensure that all officers, representatives and employees likely to receive the Confidential Information shall be under a written agreement as part of their employment or contract for work to preserve as confidential any information and knowledge which is entrusted to their employer or, in the case of a contractor, their client. The Parties shall be and shall remain liable for any breach of this clause16 by such officers, representatives and employees.

16.5 Upon the termination of this Agreement, all Confidential Information shall be returned to the Disclosing Party or destroyed at its direction. The obligations of confidentiality set out in this Agreement shall survive the termination of this Agreement.

Both parties shall ensure that they, their employees, agents and sub-Contractors shall observe the requirements of the Data Protection Act 1998 and any amendments or revisions thereto in the provision and use of the subject matter ofthe Agreement and personal data processed under it and shall comply with any

request made or direction given to the other which is directly due to the requirements of such Act.

17. ASSIGNMENT

Except upon notice to Inmarsat, Contractor shall not assign this Agreement (except an assignment solely of the right to receive monies due or to become due) or subcontract any part hereunder, in whole or in part, voluntarily, involuntarily or by operation of law without the prior written consent of Inmarsat. Any attempted assignment or subcontracting in contravention of the preceding sentence shall be void. Inmarsat may at any time, without the prior consent of Contractor, assign, transfer or novate this Agreement or any of its rights and obligations under this Agreement to its parent or any affiliated entity.

18. NOTICES

Except as otherwise provided herein, all notices or other communications herein provided to be given or which may be given by either Party to the other shall be deemed to have been duly given when made in writing and delivered in person, sent via facsimile with delivery confirmation receipt, sent via email with return receipt requested or sent via nationally recognised courier, or certified or registered United States mail, postage prepaid and addressed to the addresses set forth in the relevant Work Order.

19. PUBLICITY

19.1 Contractor agrees to submit to Inmarsat in advance of publication all advertising, sales promotion and other publicity matter relating to the Services performed by Contractor hereunder wherein Inmarsat's name or names or the name or names of Inmarsat's customers are mentioned, or language, signs, markings or symbols are used from which the connection of Inmarsat's name and any third parties' names connected therewith may, in Inmarsat's judgment, be reasonably inferred or implied; and Contractor further agrees not to publish or use such advertising, sales promotion or publicity matter without the prior written approval of Inmarsat, such approval not to be unreasonably withheld.

19.2 Contractor further agrees that Inmarsat may mention and disclose Contractor's identity and the existence of this Agreement, to its customers and potential customer, without prior consent from Contractor. In the event that Inmarsat may wish to publish Contractor's identity and associated trademark and/or logos and service marks ("Marks"), in its marketing material and advertising, it will only do so with the prior written consent of Contractor, which will not be unreasonably withheld or delayed. To the extent that Inmarsat does so use the Marks of

Contractor, Contractor hereby grants to Inmarsat non-exclusive and fully paid up license to use such Marks.

20. COMPLIANCE WITH LAWS

20.1 Contractor agrees that it will comply with all applicable federal, state and local laws, regulations and codes in the performance of this Agreement. Contractor further agrees to indemnify and hold harmless Inmarsat for any loss or damage that may be sustained by reason of Contractor's failure to comply with such federal, state and local laws, regulations and codes.

20.2 Contractor shall comply with all applicable laws, statutes, regulations and codes relating to anti-bribery and anti-corruption, including but not limited to the Bribery Act 2010 and the US Foreign Corrupt Practices Act ("FCPA") ("Relevant Requirements").

20.3 Without prejudice to the generality of the foregoing, Contractor shall:

20.3.1 not engage in any activity, practice or conduct which would constitute an offence under sections 1, 2 or 6 of the Bribery Act 2010 if such activity, practice or conducthad been carried out in the UK;

20.3.2 have and shall maintain in place throughout the term of this Agreement its own policies and procedures, including but not limited to adequate procedures under the Bribery Act 2010, to ensure compliance with the Relevant Requirements, and will enforce them where appropriate;

20.3.3 promptly report to Inmarsat any request or demand for any undue financial or other advantage of any kind received by Contractor in connection with the performance of this Agreement;

20.3.4 immediately notify Inmarsat (in writing) if a foreign public official becomes an officer or employee of Contractor or acquires a direct or indirect interest in Contractor (and Contractor warrants that it has no foreign public officials as officers, employees or direct or indirect owners at the date of this Agreement)

20.4 Contractor shall ensure that any person associated with Contractor who is performing services in connection with this Agreement does so only on the basis of a written contract which imposes on and secures from such person terms equivalent to those imposed on Contractor in this clause 20 ("Relevant Term s"). Contractor shall be responsible for the observance and performance by such persons of the Relevant Terms, and shall be directly liable to Inmarsat for any breach by such persons of any of the Relevant Terms.

20.5 Breach of this clause 20 shall be deemed a material breach of this Agreement.

20.6 For the purpose of this clause 20, the meaning of adequate procedures and foreign public official whether a person is associated with another person shall be determined in accordance with section 7(2) of the Bribery Act 2010 (and any guidance issued under section 9 of that Act), sections 6(5) and 6(6) of that Act and section 8 of that Act respectively. For the purposes of this cause 20, a person associated with Contractor includes any subcontractor of Contractor.

21. NO THIRD PARTY BENEFICIARIES

The provisions of this Agreement are set for the benefit of the Parties hereto and not for any other person.

22. WAIVERS OF DEFAULT

Waiver by either Party of any default by the other Party shall not be deemed a waiver by such Party of any other default.

23. AMENDMENTS

No provision of this Agreement or any written Work Order shall be deemed waived, amended or modified by either Party, unless such waiver, amendment or modification is in writing and signed by the authorised representative of the Party against whom it is sought to enforce such a waiver, amendment or modification.

24. ORDER OF PRECEDENCE

In the event of any conflict or inconsistency between these Terms and the provisions of any Work Order, the provisions of the Work Order shall control.

25. GOVERNING LAW

This Agreement shall be construed in accordance with the laws of England and Wales.

26. SEVERABILITY

In any of the provisions of this Agreement shall be held invalid or unenforceable, such invalidity or unenforceability shall not invalidate or render unenforceable the entire Agreement, but rather the invalid or unenforceable provision will be modified to the extent required to make it valid.

27. ENTIRE AGREEMENT

This Agreement constitutes the entire Agreement between the Parties with respectto the subject matter contained herein. Except for any Work Orders that may have been executed by the Parties hereto prior to the execution of this Agreement, all prior Agreements, representatives, statements, negotiations, understandings and undertakings are superseded hereby.

ANNEX 1 - SUPPLIER RELATIONSHIP SECURITY SCHEDULE

INFORMATION SECURITY MANAGEMENT SYSTEM

1. DEFINITIONS

1.1 The following terms shall have the meanings ascribed to them.

Access means the ability to undertake physically or logically any of the following actions:

(i) To read, copy, divert, or otherwise obtain non-public information or technology from or about software, hardware, a database or other system, or a network;

(ii) To add, edit, delete, reconfigure, provision, or alter information or technology stored on or by software, hardware, a system or network; or

(iii) To alter the physical or logical state of software, hardware, a system or network

Facility or Facilities shall mean any kind of building intended to house any Inmarsat Materials, Personal Data (as defined by the Data Protection Act) Supplier Personnel, theprovision or operation of the Services, or the Supplier's Systems Environment

Inmarsat Materials means the Company Confidential Information and the Company Data (or any of them)

Company's Systems Environment shall include, without limitation, all of the Company Group's information systems (including hardware, software, and equipment or communications devices) which are accessible to the Supplier in relation to provision ofthe Services

PCI DSS the Payment Card Industry Data Security Standard (as updated from time to time), which has been developed by the major payment card companies as the standard to be followed by organisations that process card payments

Supplier Personnel shall mean and include, without restriction, all workers whether full time, part time, contract, temporary or ancillary workers who are engaged by the Supplier, directly or indirectly, in the provision of the Services. For the avoidance of doubt this also includes personnel provided by sub-contractors used by the Supplier inprovision of the Services

Good Security Practice shall mean:

(i) the technical and organisational measures and practices that are required by, or recommended in, internationally accepted management standards and codes of practice relating to Information Security (such as ISO 27001/2); and

(ii) Security standards and guidelines (including generally accepted principles regarding the segregation of the duties of governance, implementation and control) reasonably made available to the general public or Information Security practitioners and stakeholders by generally recognised authorities and organisations regarding Information Security

ISO/IEC 27001 and ISO/IEC 27002 the international standards for Information Security management as published by the International Standards Organization and asupdated from time to time and which are:

(i) ISO 27001 Information Security Management System (ISMS) requirements; and

(ii) ISO 27002 – Code of Practice for Information Security Management

these guidelines can be followed to form the ISMS without accreditation

Information Security Policy shall mean the Information Security Policy that the Supplier shall implement and maintain in the event that the Supplier does not have its own Information Security Management Systems and which complies with the requirements of the Appendix to this Annex 1.

Information Risk, any risk that might adversely affect Information Security includingthe risk of unauthorised access or disclosure, theft, loss, destruction or misuse of Inmarsat Materials

Information Security shall mean:

(i) the protection and preservation of:

a) the confidentiality, integrity and availability of Inmarsat Materials and the Supplier's Systems Environment;

b) related properties of information such as authenticity, accountability, and non-repudiation; and

(ii) compliance with all regulations applicable to the processing of information

Information Security Management System shall mean the set of policies, processes and systems designed, implemented and maintained by the Supplier to manage Information Risk such as ISO/IEC 27001

Information Security Manager shall mean the person appointed by the Supplier with the requisite experience and expertise so as to ensure that the Supplier complies with the provisions of this Annex 1.

Supplier's Systems Environment shall include, without limitation, all information systems (including hardware, software, equipment or communication devices) owned or controlled by the Supplier (and any sub-contractors of the Supplier) which are or may be used for the provision of the Services

1.2 Capitalised terms used in this Annex 1 and which are not defined below shall have the meanings given to them in the Agreement.

2. GENERAL PROVISIONS

2.1 This Annex 1 sets out the obligations regarding Information Security with which the Supplier is required to comply when providing the Services.

2.2 The Supplier acknowledges that the Company places great emphasis on the confidentiality, integrity, security and availability of information of the Inmarsat Materials.

2.3 The Supplier will provide the Services and perform its obligations under this Agreement in accordance with:

2.3.1 this Annex 1; and

2.3.2 Good Security Practice.

2.4 The Supplier shall ensure that the Supplier's Systems Environment and the Supplier's Facilities are adequately and appropriately secured to avoid or minimise the occurrence of any Information Risk.

2.5 The Supplier will provide to the Company on request, written evidence and assurance in respect of the security of any Inmarsat Materials processed by the Supplier as may be reasonably required by the Company to comply with its obligations under the Laws.

2.6 The Supplier shall, on an ongoing basis, assess and properly manage Information Risksin all matters relating to the Services.

2.7 The Supplier shall provide assurance that Inmarsat has the right to audit and test the security controls periodically, or upon significant changes to the relationship.

INFORMATION SECURITY MANAGEMENT AND GOVERNANCE

2.8 The Supplier shall ensure that:

2.9.1 an Information Security Manager who shall be responsible for ensuring the Supplier's compliance with the requirements set out in this Agreement is appointed for the term of the Agreement; and

2.9.2 a suitable replacement deputises for the Information Security Manager when s/he is on sick or annual leave or unavailable for a period of more than 10 days.

2.9 If the Supplier operates and maintains an Information Security Management System it shall ensure that the Information Security Management System meets the requirements of Good Security Practice and includes:

2.10.1 scope statement (which covers all of the Services provided under this Agreement);

2.10.2 risk assessment (which shall include, as required, any risks specific to the Services);

2.10.3 statement of applicability (which shall be shared with, and agreed with, the Company in advance of the commencement of this Agreement);

2.10.4 risk treatment plan (which shall be shared with, and agreed with, the Company in advance of the commencement of this Agreement); and

2.10.5 incident management plan

2.10.6 it operates and maintains the Information Security Management System for the term of this Agreement.

2.10 If the Supplier does not have such an Information Security Management System in place, then the Supplier shall, throughout the term of this Agreement, comply with the requirements in the Appendix to this Annex 1.

3. INFORMATION PROCESSING & HANDLING

3.1 Without prejudice to the Supplier's obligations in respect of Data Protection in the Agreement, the Supplier shall take all reasonable precautions to:

3.1.1 ensure that Inmarsat Materials are not compromised, lost, destroyed or corrupted in any way by provision of the Services or performance of the Agreement.

3.1.2 ensure that it only uses and retains the necessary Inmarsat Materials necessary for the Company Personnel to perform the Services or its other obligations under the Agreement.

3.1.3 ensure that only those Supplier Personnel who need to have access to Inmarsat Materials for the purposes of performing the Supplier's obligations under the Agreement shall be granted access.

3.2 The Supplier shall not copy, disclose, transmit or automatically process in any manner any Inmarsat Materials or make available the same to any third party, unless expressly required by law or specifically authorised by the Company in writing.

3.3 The Supplier shall ensure that appropriate operational and procedural controls are in place to control access to Inmarsat Materials printed by any Supplier Personnel or received in hard copy format from or on behalf of the Company. All hard copy Inmarsat Materials shall be stored in a locked container when it is left unattended outside of the Supplier's standard office working hours and whenever else. It is considered that unattended hard copy information may be at risk of unauthorised access.

3.4 The Supplier shall:

3.4.1 not store or process Inmarsat Materials in, or access Inmarsat Materials from, on any service accessible to the general public e.g. DropBox, Facebook; and

3.4.2 if accessing Inmarsat Materials in a public place ensure that no unauthorised person has access to or can view such Inmarsat Materials.

4. ACCESS TO THE COMPANY'S SYSTEMS ENVIRONMENT

4.1 Where the Supplier is granted access to the Company's Systems Environment for the purpose stated in the Agreement any access to or use of the Company's Systems

Environment other than that strictly necessary for the purpose of fulfilling its obligations under the Agreement is strictly forbidden.

4.2 Access to the Company's Systems Environment shall only be permitted from a pre-agreed range of designated Supplier network addresses.

4.3 The Supplier shall ensure that access to authentication credentials (including passwords, certificates, tokens and biometric data) that enable access to the Company's Systems Environment must be kept strictly confidential by the Supplier and must not be passed on to any third party or to Supplier Personnel who are not authorised in writing for the purposes of the Agreement, unless specifically authorised to do so by the Company in writing.

4.4 All controls and limitation of access specified by the Company in relation to access to the Company's Systems Environment must be strictly complied with. Such limitations may include defining access to specific systems and times and dates of access as applicable.

4.5 The Company will, for the duration of the Agreement, provide ongoing advice as required to overcome any problems that the Supplier may have in accessing or operating the Company's Systems Environment. As such the Supplier must not attempt to resolve any problems, which, as a result, could jeopardise the Company's Systems Environment. Any problems encountered in the use of the Company's Systems Environment must be reported immediately to the Company through the agreed channels relevant to this Agreement.

5. SUPPLIER EQUIPMENT

The Supplier shall be responsible for the provision, implementation, change management, support and maintenance of the development, configuration, management and policies for all Information Security aspects of the equipment within the Supplier's Systems Environment wherever such equipment may be located.

6. ENCRYPTION

6.1 The Supplier shall ensure that technical (automatic data encryption controls for laptops and USB removable media) or procedural (policies and user awareness) controls are in place for all portable devices (e.g. laptops, tablets) and removable media (e.g. CDs, DVDs, USB storage devices, backup tapes) that contain Company Materials.

6.2 The Supplier shall ensure that Inmarsat Materials transferred electronically outside of the Supplier's Systems Environment, or over any public network, are encrypted when initiated by the Supplier.

6.3 The encryption mechanisms used in relation to Clauses 7.1 and 7.2 shall be in accordance with Good Security Practice encryption standards which would be agreed between the Supplier and the Company. Encryption functions provided by office

automation software (e.g. Microsoft Office, Adobe Acrobat) excluding Data Compression tools such as WinZip (where 256 AES encryption or higher is used) must not be relied upon to protect Inmarsat Materials unless specifically agreed in writing with the Company.

7. SECURE DISPOSAL OF INMARSAT MATERIALS

7.1 The Supplier shall immediately destroy or delete, in accordance with Good Security Practice, Inmarsat Materials when no longer required and in the event oftermination in support of the Services being provided.

7.2 Any Inmarsat Materials which are no longer needed shall be treated as confidential waste. The Supplier shall:

7.2.1 securely destroy or dispose of all such Inmarsat Materials and if the Inmarsat Materials reside on any item of hardware that is being disposedof, prior to the disposal of the hardware item; and

7.2.2 provide independently verifiable evidence that all such media has been processed in accordance with Good Security Practice to ensure the data contained on it cannot be subsequently retrieved.

8. SECURITY INCIDENTS

8.1 In the provision of Services to Inmarsat and as part of the security incident response procedure, if the Third Party becomes or is made aware of any contravention of the information security requirements under the Contract, or of unauthorised access to Inmarsat's information or any Inmarsat's Systems including Inmarsat network, the Third Party shall (and shall ensure that its Sub-Supplier shall):

8.1.1 Immediately report the incident to Inmarsat;

8.1.2 Promptly provide Inmarsat with a detailed written report setting out the details ofand reasons for the contravention of the information security requirements and describing in detail any Inmarsat's Information, Systems and/or Inmarsat's Systems which have been accessed without authorisation;

8.1.3 Provide Inmarsat, at no additional cost, with any assistance to restore Inmarsat Information, the Systems and Inmarsat's Systems and any other assistance thatmay be required by Inmarsat;

8.1.4 Preserve evidence to include collection, retention and presentation of such evidence to Inmarsat;

8.1.5 Promptly return to Inmarsat any copied or removed Inmarsat's Information;

8.1.6 comply with all reasonable directions of Inmarsat; and

8.1.7 Take immediate remedial action to secure Inmarsat Information, Systems and /or Inmarsat's Systems and to prevent reoccurrences of the same or similar contravention and provide Inmarsat with details of such remedial action.

8.2 If either a criminal situation or a breach of Third Party policies and the requirements inthe Contract occurs involving Third Party or Subcontractor personnel who are providing Services to Inmarsat and such criminal situation or breach becomes known to the Third Party (or its Sub-Supplier), Inmarsat must be notified as soon as practicable of the facts surrounding the same.

9. PCI DSS

9.1 Should Services under this Agreement require the Supplier to obtain, store or process payment card data in-scope for PCI DSS the Supplier:

9.1.1 shall do so in compliance with the most up-to-date Payment Card Industry Data Security Standards which are put in place from time to time by the PCI Standards Council, details of which are available from https://www.pcisecuritystandards.org/security_standards/index.php to the extentthat PCI DSS applies to them by virtue of any such transfer, storage or connection;

9.1.2 shall restrict the disclosure of the Payment Card Information to those of its employees who may be required by it to assist it in meeting its obligations underthis Agreement;

9.1.3 warrants that it is PCI DSS compliant and indemnifies the Company Group for any fine, levy or sanction imposed on the Company Group for any non-compliance with the PCI DSS regulations made by any court, payment brand or payment aggregator or card issuer; and

9.1.4 will supply to the Company, on request, summary of any gap analysis, QSA report or remediation action plan that demonstrates its compliance with PCI DSS.

9.1.5 Will supply to the Company, on request, shall provide to Inmarsat, written details around any compensating controls employed by the Third Party to achieve risk mitigation in technical areas which do not meet the PCI DSS requirements.

9.2 For the avoidance of doubt, Supplier shall only carry out any such transfer or storage where it is reasonably necessary for carrying out of the relevant part of the Support Services.

10. AUDIT AND COMPLIANCE BY THE SUPPLIER

10.1 Where the Supplier's Systems Environment is connected to the internet or to other organisations/networks (including the Company's System Environment), the Supplier shall perform a security penetration test to ensure the system's security at least annually and upon any major changes to the Supplier's Systems Environment that could have a security impact to the Supplier's Systems Environment.

10.2 The Supplier shall perform risk based security audits of the Supplier's System Environment at least once every twelve months and upon many major changes to the Supplier's Systems Environment.

10.3 If the Supplier provides a code or software development service to the Company the Supplier shall be required to follow Good Security Practice for code or software development within the Supplier's Systems Environment.

10.4 If the Supplier provides a system development service to the Company the Supplier shallbe required to follow Secure system development within the Supplier's Systems Environment.

10.5 Should Services under this Agreement require the Supplier to provide software development Services, Supplier and the Company will mutually agree code development practices in the Engagement letter prior to this Services being executed.

10.6 If an investigation or audit is conducted by Inmarsat or on behalf of Inmarsat, the Supplier (and its Sub-Supplier) will ensure that all personnel shall cooperate with suchinvestigators or auditors and, if requested, will make relevant personnel available for interview.

10.7 If the Third Party has attained external validation or certification to any security industry standards, for example, this may include certification or standards such as ISO 27001, PCI DSS, SSAE 16 or FSA, or any other audit standards which may contain security control assessments, the Third Party shall provide evidence of the relevant certification and/or Statement of Applicability upon request.

11. TERMINATION OF AGREEMENT

11.1 Upon expiry or termination of the Agreement for any reason, in addition to the termination provisions as set out in the Agreement, the Supplier shall, within eight (8)weeks' of such expiry or termination also:

11.1.1 return, or securely destroy in accordance with Section 8, all Inmarsat Materials, except that which it is required to retain for legal or regulatory compliance obligations or its internal compliance procedures. Where this is the case, it must

remain secured in accordance with the other requirements of this Annex 1 and be returned or securely disposed of in accordance with Good Security Practice assoon as the legal or regulatory compliance obligations expire;

11.1.2 where Inmarsat Materials are securely destroyed, the Supplier shall provide independently verifiable evidence of this and a certification from an officer confirming that such destruction has been carried out.

11.2 Notwithstanding paragraph 11.1, the Supplier will be permitted to retain one (1) copy of Inmarsat Materials for the purposes of and for so long as required by any law or regulatory requirement or judicial process.

APPENDIX 1

Where the Supplier does not have an Information Security Management System, they shallcomply with the following provisions.

1. RISK ASSESSMENT

1.1 The Supplier shall carry out a risk assessment to assess the Information Risks specific tothe nature of the Services being provided to the Company and to define any specific information security and data handling arrangements that are applicable to this. The Supplier shall also:

1.1.1 consider each of the requirements set out below as part of this risk assessment;and

1.1.2 share the outcomes of the performed risk assessment with the Company and mutually agree any specific information security and data handling arrangements under the Letter of Engagement between the Supplier and the Company.

2. PHYSICAL ACCESS TO FACILITIES

2.1 The Supplier shall:

2.1.1 maintain appropriate and adequate physical access control mechanisms to prevent unauthorised access to Supplier Facilities in accordance with Good Security Practice;

2.1.2 ensure that it puts in place and operates physical access control mechanisms to prevent Supplier Personnel entering areas within the Supplier's Facilities that theyare not authorised to enter;

2.1.3 ensure that physical access controls mechanisms within the Supplier's Facilities for communications rooms, server rooms or any rooms providing connectivity or transport for the Company's Materials shall prevent unauthorised Supplier Personnel or other individuals from entering these locations, including ensuring that:

(a) entry points into data centres shall be accessed via use of authentication which is unique to the individual accessing the location. (i.e. shared PIN codes or keys are not permitted); and

(b) entry points into other locations shall be accessed by only those authorised to have access to the location for business purposes.

2.1.4 ensure that entry and exit points to Supplier Facilities, data centres and server rooms for the Company's Materials are monitored by CCTV (24x7). CCTV images shall be retained for a minimum of 30 days.

2.2 ensure that any third party requiring access to provide support or maintenance for any equipment that is directly or indirectly involved in providing the Services shall be logged into and out of the Supplier's Facilities including the reason for their visit and the responsible member of Supplier Personnel and shall be escorted by the responsible member of Supplier Personnel at all times;

2.3 ensure that logs will be maintained of access to the Supplier's data centres and that these logs are retained for at least 6 months;

2.4 ensure that data centre and server room locations must be constructed of floor to ceilingwalls and either not contain windows or where windows are present these must be opaque and secured by suitable grills/bars to prevent physical ingress into the location; and

2.5 ensure that fire doors on security perimeters to the Supplier's data centre and server room facilities should be alarmed and should close shut.

2.6 Where Inmarsat to agree (either under the Contract or by prior written consent) to the Third party to provide the Services from a shared Site, the Third Party shall as a minimum:

a. Segregate the area in which the Services are performed for Inmarsat;

b. Implement a clearly defined area for performing the Services;

c. Ensure that the Services and facilities required to provide the Services to Inmarsat are kept completely physically separate from the Third Party's other

clients with dedicated exit/entrance points and clear divides as defined bypartition walling or desk plans.

3. ACCESS CONTROL

3.1 All Supplier Personnel who access the Supplier's Systems Environment must be granted authorised access using formally defined and approved processes in accordance with Good Security Practice.

3.2 All Supplier Personnel must be allocated a unique identifier for their personal and soleuse.

3.3 The Supplier shall ensure that Supplier Personnel activities can subsequently be traced back to the responsible individual.

3.4 The Supplier must promptly remove, or request the Company to remove, the access rights of any Supplier Personnel who have changed role or left the Supplier's employment or who no longer need access to the Company's Systems Environment and / or the Supplier's Systems Environment for the purposes of the Agreement.

3.4.1 The Supplier must periodically check for and remove, or in the case of the Company's Systems Environment request the Company to remove any redundant user identifiers and accounts relating to Supplier Personnel that are no longer needed in relation to the Supplier's Systems Environment or the Company's System Environment. The Supplier must keep a formal record of the checks carried out and these checks must be performed at least annually.

3.5 The Supplier must not reallocate user identifiers issued to specific Supplier Personnel to other Supplier Personnel.

3.6 The Supplier must maintain a formal record of all Supplier Personnel authorised to have access to the Company's Systems Environments, which must be subject to regular review (at least quarterly) and must provide the Company with a copy of the record upon request.

4. SUPPLIER EQUIPMENT

4.1 The Supplier shall implement a formal change management process to ensure changes made to the Supplier's Systems Environment are approved before being implemented.

4.2 Any change to the Supplier's Systems Environment which does or may reduce specific security control requirements defined in an Engagement letter for a specific project shallbe subject to the Company's prior written approval.

4.3 The Third Party shall ensure that all changes for information systems, upgrades, and new software in relation to the Services have considered security control requirements, based upon the identified risks, and that these changes are tested prior to implementation.

4.4 The Supplier shall ensure that regression steps are documented prior to implementing the change.

4.5 Firewall and network based intrusion detection software must be implemented to control and monitor connections to the Supplier's Systems Environment from the Internet or other networks.

4.6 All information security controls relating to the development, build, configuration, deployment, operation, change management, maintenance and support for all technologies relating to the Supplier's Systems Environment shall be in line with Good Security Practice.

4.7 The Supplier shall ensure that all systems within the Supplier's Systems Environment or accessing the Company's System Environment have appropriate up to date anti-virus software installed, in accordance with Good Security Practice. Anti-virus software updates must be applied upon being released by the vendor and the software must be configured for at least daily Standard and on-access scanning.

4.8 Devices (including PCs, laptops and servers) which are used to access, hold or process Inmarsat Materials or devices which are used to service, support or maintain systems holding or processing Inmarsat Materials must:

4.8.1 ensure user interface screens or sessions automatically lock after a short period of inactivity (maximum 30 minutes) and require use of a password, or other authentication credential, to unlock;

4.8.2 have all vendor operating system and application software updates / patches installed promptly upon issue by the vendor;

4.8.3 have all successful and unsuccessful logon attempts and modifications to system access permissions logged and these logs must be retained for at least 90 days unless the frequency of security events and reasonable file size restrictions reduce this retention period during a specific time period.

4.9 The Supplier shall ensure that Inmarsat Materials obtained from the Company's production System Environment or relating to Company customers or personnel is only stored and processed in the Supplier's production Systems Environment.

5. SUPPLIER PERSONNEL

5.1 The Supplier shall ensure that all Supplier Personnel shall be appropriately vetted for security compliance relevant to the Services being provided to the Company before commencement of the individuals' involvement with the Services. This vetting shall be incompliance with any legal or regulatory requirements applicable to the Services.

5.2 Should Services under this Agreement require Supplier Personnel to have Access to download/export significant volumes of Inmarsat Materials, i.e. Supplier Personnel holding privileged levels of Company system access such as system administrators, database administrators, Supplier vetting checks may include and not be limited to:

5.2.1 verification of employment references covering the previous three years employment. If there is no such previous employment history then two professional character references may be verified instead;

5.2.2 a check for completeness and accuracy of the applicant's CV or employment application form;

5.2.3 confirmation of professional and academic qualifications;

5.2.4 a criminal records check, subject to local laws, regulations and privacy requirements permitting these checks, in addition to the practicalities and feasibility to check existing staff; and

5.2.5 an identification check, for example via a passport or birth certificate.

5.3 The Supplier shall maintain complete records of the checks performed for each person vetted.

6. AWARENESS & TRAINING

6.1 The Supplier shall ensure that all Supplier Personnel complete an information security awareness training programme.

6.2 The information security awareness programme shall:

6.2.1 ensure Supplier Personnel are aware of their obligations in relation to protectingthe confidentiality, integrity and availability of Inmarsat Materials;

6.2.2 ensure Supplier Personnel are made aware of relevant Supplier information security policies;

6.2.3 be performed:

(a) before Supplier Personnel are given access to the Company's Systems Environment and / or Company Data or Company Confidential Information; and

(b) at regular intervals thereafter, such intervals to be no more than twelve months.

6.3 The Supplier shall ensure that Supplier Personnel shall only be involved in the provision of the Services or parts of the Services for which they have been adequately trained.