Es'hailSat Policy
INFORMATION AND TECHNOLOGICAL SECURITY

Part A – CYBER SECURITY

The Products are designed to comply with a variety of network security best practices and standards such as the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, and the International Standard ISO/IEC 17799:2000 Code of Practice for Information and Security Management.

Compliance with these standards is intended to enable the end-user to transport sensitive data over a trusted network. To provide a common understanding of terminology used throughout Part A of this Annex, the following definitions are provided. These definitions only apply to Part A of this Attachment 2.

Definitions:

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Availability: Ensuring timely and reliable access to and use of information.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Information Assurance (IA): Measures that protect and defend information and information systems by ensuring their availability, Integrity, Authentication, Confidentiality, and Non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Non-repudiation: Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

Subscriber Data: Any data created, stored, and/or traversing the Customer's Subscriber Virtual Network (SVN) data channel originating with or being received by the end user.

1. **Security Services Provided**

The baseline network for provision of the Products (to include the Satellite Terminals, Satellite Access Station, and Data Communications Network, infrastructure components) is designed to be capable of meeting security requirements equivalent to those assigned against the NIST 800-53 Low-Impact baseline control set. Security requirements above this can be provided through additional service offering contracts, as detailed in [Annex 4 - Interconnect]. Es'hailSat will provide reasonable assistance to the Subscribers and Customers that contract for such additional security provision in their efforts to establish self-assessments, audits, and tests of such additional security provision.

2. **Service Standards of Use:**

The Customer shall ensure that the benefits and obligations of the following provisions are adequately conveyed to its customers for the provision of Products and such provisions are adequately conveyed to the Customer's Service Providers and Subscribers.

2.1. Es'hailSat automatically accesses and records core module information, SIM Card and Satellite Terminal settings (as applicable) for the purpose of Satellite Terminal and SIM Card identification and billing. The Customer shall permit, and shall procure that Service Providers and Subscribers agree to permit, Inmarsat's Network Management System to access the core module and SIM Card (as applicable) and to monitor, adjust and record such profiles and settings as required for the purpose of providing the Products. The core module and SIM Card: contains a security certificate used for authenticating a Satellite Terminal on the Inmarsat Network; collects usage statistics; and contains configuration parameters that make up that Satellite Terminal configuration. The Customer consents and shall procure that Service Providers and Subscribers also consent, to Inmarsat monitoring network connection and network performance, and to Es'hailSat accessing and adjusting Satellite Terminal settings, as they relate to the Products. Es'hailSat does not share information collected for the purpose of network performance monitoring or for providing customized technical support outside of Es'hailSat or its Affiliates.

2.2. Es'hailSat provides data Confidentiality as between Subscribers through virtual private network segments traversing the Inmarsat Network. However, the Customer agrees, and shall procure that Service Providers and Subscribers agree, to be responsible for maintaining the security of their Satellite Terminals and Subscriber Data, including without limitation, encryption of Subscriber Data and protection of their user ID, password and personal data. If the Customer, Service Providers or Subscribers believe their login credentials have been lost or stolen, that someone has gained access to their account or login credentials without permission, or their terminal device has been compromised in any way, the Customer shall, and shall procure that the Service Providers and Subscribers shall, immediately contact Es'hailSat customer service desk.

2.3. The Customer shall ensure the Subscriber is solely responsible for management of its Subscriber Data, including but not limited to back-up and restoration of that data. The CUSTOMER AGREES THAT Es'hailSat IS NOT RESPONSIBLE FOR THE LOSS OF CUSTOMER, SERVICE PROVIDER, OR SUBSCRIBER DATA OR FOR THE BACK-UP OR RESTORATION OF SUBSCRIBER DATA.

2.4. Es'hailSat does not permit any unplanned security vulnerability testing or tools to be deployed on the Inmarsat Network by any entity. Any attempt at unplanned vulnerability scanning or testing will be seen as a potential network penetration attempt and be immediately blocked - which may affect provision of the Products. In such circumstances, Es'hailSat shall not be liable for any effect on the provision of the Products. Es'hailSat does conduct routine vulnerability testing of the Inmarsat Network infrastructure. Additional information regarding security posture and/or services must be directed to Es'hailSat customer service desk.

2.5. The Customer shall ensure all IA certification, accreditation, and evaluation activities relating to the Products are the responsibility of the Subscriber. Any information requests for security standards compliance must be directed to Es'hailSat customer service desk.

Part B – TECHNOLOGICAL FRAUD PREVENTION PROCEDURES

1. **General Requirements**

1.1. The Parties shall assist legitimate Subscribers whose Satellite Terminal(s) may be compromised by technological fraud, including, without limitation, by promptly doing the following:

1.1.1. the Customer shall (with the reasonable assistance of Es'hailSat upon request), contact such Subscribers to inform them of the existence of the fraud;

1.1.2. the Parties shall assist such Subscribers with obtaining replacement Satellite Terminal(s)/core module(s)/SIM Cards (as applicable); and

1.1.3. the Parties shall provide general information concerning fraud avoidance.

1.2. In the event that a Subscriber must replace its Satellite Terminal, SIM Card and/or core module as the result of technological fraud arising from the failure of the Customer to comply with these Technological Fraud Prevention Procedures then the Customer shall reimburse Es'hailSat for administrative costs associated with such deactivation and reactivation and costs incurred by the Subscriber in connection therewith (provided that in both cases such costs shall be demonstrated to be reasonably incurred).

1.3. The Customer shall:

1.3.1. submit (and provide updates when necessary) to Es'hailSat the name(s) and contact numbers of at least two persons who are authorised by the Customer to:

1.3.1.1. receive from Es'hailSat, notification and information on fraud and suspected fraud;

1.3.1.2. act on the information received;

1.3.1.3. bar/unbar, suspend/unsuspend and activate/deactivate any blockings on Satellite Terminals or SIM Cards (as applicable) that have been implemented following the detection of Technological Fraud;

1.3.1.4. request a Satellite Terminal or SIM Card (as applicable) that has been involved in Technological Fraud to be added to Es'hailSat's maintained "Black List";

1.3.1.5. provide additional information that may be used in the investigation of fraud to Es'hailSat. Such information can include, for example, the IP services used, destination IP addresses accessed, 'called' or 'dialled' numbers, etc.;

1.3.1.6. provide reasonable proof to Es'hailSat that the fraud has been committed; and

1.3.1.7. keep Es'hailSat informed of any changes to the contact details.

1.3.2. notify Es'hailSat immediately of any proven or suspected case of Technological Fraud;

1.3.3. release to the appropriate authorities, on a confidential basis and subject to national law, all commercial and operational data relevant to the investigation of any case of fraudulent use of the system;

1.3.4. implement operational procedures relevant to the management and monitoring of fraud, including the implementation of specific recommendations and measures from time to time in accordance with the Agreement;

1.3.5. not provide Products to a Satellite Terminal and/or SIM Card (as applicable) that the Customer knows or has reason to believe is fraudulent or fraudulently operated;

1.3.6. implement appropriate and commercially reasonable security measures that will limit access to the physical and logical location and identity of the Satellite Terminal ID, SIM Card, Subscriber details, service plans and other related service activation information;

1.3.7. immediately notify Es'hailSat of any breach of security and provide details of any sensitive data which may have been compromised;

1.3.8. following notification by Es'hailSat of suspected technological fraud, or suspicious changes in behavioural patterns, initiate investigations, respond to Es'hailSat within 24 hours of such notification and keep Es'hailSat informed of the progress of those investigations;

1.3.9. assist Es'hailSat in a timely manner in investigating technological fraud committed against the Inmarsat Network which may include:

1.3.9.1. contacting the owner or operator of the Satellite Terminal and/or SIM Card (as applicable) to verify any suspected fraudulent usage;

1.3.9.2. providing applicable information which may include IP services used, destination IP addresses accessed, 'called'/'dialled' numbers, country of call destination (where release of such information is permitted) and other relevant information that may facilitate the resolution of fraud; and

1.3.9.3. facilitating, where practical and permissible, the use of Satellite Terminal ID, core module DID, PoP, APN or other Customer resources associated with the Inmarsat Network in order to monitor fraudulent activities;

1.3.10. where permissible, under the applicable national law and regulation, provide information that could help Es'hailSat to identify any Satellite Terminal, SIM Card or core module clone;

1.3.11. ensure that Service Providers comply with the Technological Fraud Prevention Procedures set out in this Attachment 2; and

1.3.12. cooperate with Es'hailSat to develop additional, cost-effective technological fraud prevention procedures in the future.

1.4. Es'hailSat shall:

1.4.1. notify the Customer promptly of any proven or suspected case of fraudulent use of the Inmarsat Network or Products relevant to the provision of the Products to the Customer, except where a reasonable delay is required by Es'hailSat in order to rectify or confirm the existence of such fraudulent use;

1.4.2. provide such notification primarily by electronic message. The effective date of the notification shall be the date when the electronic message was sent;

1.4.3. provide reasonable assistance to the Customer in providing operational data to the appropriate authorities, on a confidential basis and subject to national law, relevant to the investigation of any case of fraudulent activity;

1.4.4. implement operational procedures relevant to the management and monitoring of fraud, including the implementation of specific recommendations and measures from time to time in accordance with the Agreement;

1.4.5. promptly on becoming aware notify the Customer of any breach of security and provide details of any sensitive data deemed by Es'hailSat to be specifically relevant to the Customer operations which may have been compromised; and

1.4.6. provide reasonable assistance to the Customer in a timely manner in investigating Technological Fraud.