CHAPTER B16—STANDARD AGREEMENT FOR SIS PARTICIPATION

This SIS Participation Agreement ("**Agreement**") is entered on _____("**Effective Date**")
by and between [Company]_____
a company incorporated under the laws of [Country/State]_____
with its head office located at: _____
_____
_____
_____

("**Participant**") and the **INTERNATIONAL AIR TRANSPORT ASSOCIATION,** an association incorporated by Special Act of the Parliament of Canada, with its head office at 800 Place Victoria. P.O. Box 113, Montreal, Quebec, Canada, H4Z 1M1 ("**IATA**") (each a "**Party**" and collectively, the "**Parties**").

PREAMBLE

WHEREAS IATA is an international association of airlines that promotes safe, regular and economical air transport and facilitates collaboration among air transport enterprises engaged directly or indirectly in international air transport services;

WHEREAS IATA operates and manages one or more industry clearing houses as a service to the airline industry on a cost recovery basis;

WHEREAS in 2007, to enhance the efficiency and reduce the cost of clearing house operations, IATA has developed an integrated billing and settlement solution to operate on a paperless basis and simplify existing processes (the "**SIS Project**");

WHEREAS the information technology solution resulting from the SIS Project to provide the air transport industry simplified, enhanced and optimized IATA settlement systems consists of:

(i) streamlining and integrating the industry settlement systems into a single coherent settlement process that can handle each and all types of billing (passenger, cargo, UATP, miscellaneous/non-transportation) including such as original billings, rejections, billing/credit memos and correspondence;

(ii) adding electronic invoicing and support functionalities and services to reduce the cost of settlement, and

(iii) making all of these enhancements available to all other air transport industry settlement processes involved in or forming part of the industry settlement systems (such as industry clearing houses) (all together "**SIS Solution**");

WHEREAS IATA operates and provides the SIS Solution, the Service and the Additional Services (both terms Service and the Additional Services are defined below) from various locations worldwide, including through the use of subcontractors;

WHEREAS The Parties now wish to set out the terms and conditions pursuant to which IATA has agreed to provide the Service and Additional Services to Participant, and Participant has agreed to accept the Service, and may elect to choose Additional Services, in exchange for certain fees, and where the Participant recognizes that IATA operates the Service and any Additional Services through sub-contractors worldwide not with the intent of generating profits and, to the extent practicable, essentially on a cost recovery basis, the whole as further set forth below; and

WHEREAS the Parties understand and agree that IATA's willingness to perform the Services and the Additional Services on a cost recovery basis hereunder was and is a material factor in making the Parties agree to the terms and conditions herein, including in particular the provider-limited liability regime set forth in this Agreement.

This Preamble shall form an integral part of this Agreement.

NOW THEREFORE THE PARTIES SIGNING THE VARIOUS COUNTERPARTS HEREOF AGREE AMONGST THEMSELVES AS FOLLOWS:

1. SUBMISSION OF ELECTRONIC INVOICE DATA VIA ELECTRONIC DATA INTERCHANGE (EDI) FOR THE PURPOSE OF INTERLINE BILLING

1.1 The Parties agree to submit and receive (as applicable) electronic interline invoices in accordance with the procedures and standards set out in this Agreement.

1.2 The provisions of this Agreement are in addition to the procedures set out in the IATA Revenue Accounting Manual ("**RAM**") and the Airline Clearing House ("**ACH**") Manual of Procedure as amended from time to time.

1.3 This Agreement includes the Attachments A, B, C, D, E, F and G which may be amended in accordance with this Agreement, and published by IATA from time to time.

1.4 IATA shall enter into agreements with additional airlines, suppliers and other related parties for the provision of the Service and Additional Services ("**SIS Participants**") only on the same standards, terms and conditions as set out herein.

1.5 Whenever used in this Agreement "**includes**" and "**including**" mean "including (or includes) without limitation".

2. PROVISION OF SERVICE

△ 2.1 As of the Effective Date and during the Term of this Agreement, IATA shall be responsible for providing to the Participant, and Participant agrees to use the Simplified Invoicing and Settlement (SIS) services described in the Attachment D (the "**Service**")

2.2 Participant may also elect to use certain additional services in accordance with the Attachment B ("**Additional Services**").

3. PARTICIPATION IN THE SERVICE

3.1 Obligations and Responsibilities of the Participant

3.1.1 Participant shall pay IATA the fees and charges set out in Section 8 for the provision of the Service.

3.1.2 If Participant elects to use any Additional Services it shall pay IATA the fees and charges set out in Section 8 for the provision of such Additional Services as selected in Attachment B.

3.1.3 Participation in this Agreement is conditional upon Participant agreeing that IATA will be generating electronic invoices on the Participant's behalf, and on agreeing to accept electronic invoices from all other SIS Participants. Invoices are deemed to be received as soon as notification has been sent to the Participant. It is the Participant's responsibility to secure any permissions or authorizations that may be required in their country or countries of base regarding the use of electronic invoices, and to comply with laws that those countries may apply to the creation of invoices, determination of applicable taxes, management of access controls, record keeping and legal archiving. The correctness of any data submitted to the Service and/or Additional Services remains the responsibility of the Participant at all times. Where electronic signatures have been requested, the Participant authorizes IATA to apply or validate the electronic signature through the electronic signature service providers listed in Attachment D and as amended from time to time.

3.1.4 Participation is conditional upon preliminary testing and successful completion of the certification process for the file types that Participant intends to submit.

3.1.5 Settlement of invoices entered into the Service will be made directly by the debtor to the creditor using such channels as may have been agreed between them. Where settlement is to be effected through an industry clearing house, each SIS Participant must have access to and act in compliance with the rules of a clearing house.

3.1.6 The Participant acknowledges that settlement of electronically submitted invoices via the Service could generate an automatic default notice if payment is made by any Participant not based on the gross amount of the invoice, but on the gross amount net of deduction or withholdings based on taxes or other governmental charges.

△ 3.1.7 In supplying Data (as further defined) and any other data to be included in the Service and Simplified Invoicing and Settlement (SIS) system ("**System**"), the Participant shall comply with the procedures and standards provided for in this Agreement. All invoice data supplied must be transmitted in compliance with the published IS-XML or IS-IDEC standards as valid at the time, or be entered by the Participant via the user interface provided. The Participant shall maintain in the System a full and up to date list of the names of persons authorized by it to supply, modify, or withdraw data on its behalf or to issue instructions concerning the applicability or distribution thereof. IATA will make all reasonable efforts to conform to the Participant's instructions in a timely manner.

3.1.8 Where a Participant has issued an electronic invoice that it believes to be in error, it must promptly notify IATA and the designated recipient, and take the necessary steps to correct the situation in accordance with the procedures described in the RAM, the ACH Manual of Procedure and/or other clearing house procedures, as applicable.

3.1.9 The Participant holds the entire responsibility for the accuracy and the completeness of the tax and VAT-related information it provides to IATA and third parties in connection with the Service. When national legislations provide for specific validation procedure for the tax or VAT identification number of the customer, the obligation to perform such validation remains with the Participant.

3.1.10 It is the sole responsibility of the Participant to ensure the Data or any other information transmitted via the Service and/or Additional Services is in compliance with applicable laws, including applicable privacy laws. To the extent applicable, any payment card data supplied under the Service by the Participant or any third party acting on its behalf shall be masked in accordance with Payment Card Industry Digital Security Standard (PCI-DSS) specifications using the format 123456XXXXXX7890.

3.2 Personal Data

IATA may receive Personal Data (as defined below) under this Agreement from the Participant or its employees. IATA shall process such Personal Data solely as needed for the performance of the Service and/or Additional Services. Furthermore, in accordance with EU Directive 95/46/EC, if requested by Participant, the Parties shall sign the EU Standard Contractual Clauses, as attached hereto as Attachment G, pursuant to which IATA may transfer the Personal Data to its subcontractors on condition that such subcontractors have entered into the same obligations. "**Personal Data**" means any data, which permits the identification of an individual. IATA hereby notifies Participant of such processing and Participant hereby grants consent required for the processing of Personal Data. Participant agrees that IATA shall not be in breach of this Agreement if IATA refuses to perform any transaction offered as part of the Service and/or Additional Services described in this Agreement to Participant when Participant's employee, agent and/or representative refuses to consent to the processing of its necessary Personal Data for the performance of such transaction(s).

3.3 For the purpose of this Agreement "**Data**" includes all information (including Personal Data) to be provided to or otherwise made available to or processed by the System, the SIS Solution, the Service, the Additional Services or IATA, by the Participant or any third party acting on its behalf for purposes of or in relation to this Agreement, the SIS Solution, the Service or the Additional Services.

4. GENERAL ADMINISTRATION OF STANDARD AGREEMENT

4.1 The general administration of this Agreement shall be undertaken by IATA.

4.2 The cost of administering the Service is met by charging a combination of a participation fee plus transaction fees in accordance with the Pricing Schedule in Attachment A and as amended from time to time in order to recover Service operating costs.

4.3 All communications from the Participant concerning this Agreement shall be addressed to IATA. All communications from the Participant concerning problems in the delivery of the Service and/or Additional Services should be referred to the help desk as detailed in Attachment E.

4.4 IATA may undertake any study, and perform any other acts, that are designed solely to develop and improve the Service at no cost to the Participants unless otherwise agreed with the SIS Steering Group.

4.5 Any failure identified in the provision of the Service will be directed in the first instance to the designated help desk as provided in Attachment E, which shall log the failure and identify the action required.

△ 4.6 Each Participant shall file a signed copy of this Agreement with IATA, together with a schedule of dates outlining when the Participant will implement Simplified Invoicing and Settlement (SIS) processes for each clearing house transaction category. IATA Revenue Accounting will publish, in the form of Attachment F to this Agreement, the names of the SIS Participants that are participating in the "**Service**" and in which clearing house transaction categories they participate. In the case of SIS Participants that are members of the ACH, IATA will also notify the ACH Secretary-Treasurer, who will publish to ACH members.

5. GOVERNANCE

5.1 The Service is governed by the groups referred to below and described in Attachment C.

5.2 IATA shall hold a general meeting of the SIS Participants annually, and additional general meetings shall be held at any time at the discretion of IATA or on the request of a majority of SIS Participants ("**SIS General Meeting**").

5.3 A written notice of the intention to hold such SIS General Meeting shall be communicated by IATA to the SIS Participants not less than three (3) months before the date scheduled for such SIS General Meeting. Agenda items must be submitted at least forty-five (45) days before the date of such meeting, and the agenda will be issued thirty (30) days before the date of such meeting.

△ 5.4 Voting will take place at the SIS General Meeting to elect five (5) representatives to the SIS Steering Group for a term of three (3) years. Nominations shall be made to IATA before the date of the meeting, at which the nominees must be present. The Participants will elect the representatives by majority vote.

5.5 In IATA or SIS Steering Group's opinion, when elections or other measures require action by Participants outside the schedule of SIS General Meetings, Participant agrees that a mail vote may be taken as an alternative.

6. MODIFICATIONS

6.1 Amendments to System functionality may be submitted as a proposal to the SIS General Meeting duly convened in accordance with paragraph 5.2 and shall be referred initially to the SIS Steering Group for review. If accepted by the SIS Steering Group they will be referred to SIS Operations (as defined in Attachment C) for analysis and costing. SIS Operations will then develop the specifications. The final agreed proposal shall be submitted to the SIS Steering Group for approval. Changes to system functionality may be proposed by the Participants at any time before the deadline of the SIS General Meeting. Major changes to system functionality must be approved by IATA to ensure operational efficiency.

6.2 Amendments to System functionality as a result of industry mandated changes shall be initiated by the SIS Steering Group and referred to SIS Operations for review and costing. SIS Operations will then develop the specifications. The final agreed proposal shall be submitted to the SIS Steering Group for approval.

6.3 Amendments to the then current Agreement which are accepted by IATA and agreed by seventy five percent (75%) of those present at the SIS General Meeting, duly convened in accordance with paragraphs 5.2 and 5.3 shall become effective and shall be applied by all SIS Participants, as from a date which shall be determined by the SIS Participants present and entitled to vote at the SIS General Meeting.

6.4 To be eligible to vote for changes to this Agreement with Attachments, the Participant must be transmitting and receiving invoices through the Service.

6.5 Where changes to the RAM, ACH Manual of Procedure, or other industry rulings require changes to this Agreement, the SIS Steering Group is empowered to agree to the appropriate amendments to this Agreement. The SIS Steering Group shall notify the Participants of all amendments, giving their date of effectiveness.

6.6 In addition, when IATA's review of an operational and/or individual Participant problem suggests that an editorial change would improve understanding, IATA may make editorial amendments provided they do not change the intent of the Agreement and/or procedures. Editorial amendments that do not change the intent of the Agreement and/or procedures will be notified via the RAM. IATA will notify the ACH Secretary-Treasurer.

6.7 All changes and amendments made in accordance with paragraphs 6.5 and 6.6 above will be submitted to the next SIS General Meeting for final ratification.

7. SERVICE LEVEL

7.1 General

The level of performance of the Service shall be at least consistent with the service levels described in Attachment E ("**Service Levels**").

7.2 Failure to Perform

In the event IATA fails to meet any Service Level requirement, IATA shall, or shall cause its sub-contractor to, (i) investigate the causes of such failure; (ii) take the necessary measures to correct such failure within the time frames set forth in Attachment E and start implementing the corrective measures, and (iv) take appropriate preventive measures so that such failure does not reoccur.

7.3 Service Level Credits

Any Service Level credit available to IATA will be applicable for the benefit of all SIS Participants and/or the industry. Such Service Level credits shall not be Participant's exclusive remedy for any failure to meet the Service Levels; however, any amount of Service Level credits effectively received by Participant will be deducted from monetary damages recovered by Participant from IATA as a result of an event also giving rise to a Service Level credit. The balance of any such monetary damages will be recoverable under Section 13.

7.4 Measurement and Monitoring Tools

7.4.1 IATA will monitor that the provision of the Service and Additional Services is in accordance with the Service Levels described in Attachment E. IATA shall use the necessary measurement and monitoring tools and procedures required to measure the performance of the Service and Additional Services against the applicable Service Levels.

7.4.2 Each Service Level shall be measured on a monthly basis and reported to the SIS Steering Group quarterly, unless stated otherwise in Attachment E. IATA shall, upon request of the Steering Group, provide reports at a sufficient level of detail, to verify the Service performance and compliance with the Service Levels. This data shall be provided to the Steering Group, and shall be considered Confidential Information. For the avoidance of doubt, any such report shall not contain any Data (as defined below).

8. FEES AND CHARGES

8.1 Fees and charges for the Service and the Additional Services as described in Attachment A will be paid by the Participant for the Service and/or the Additional Services.

8.2 The fees and charges do not include, communication charges relating to the Participant's transmission of input or receipt of output files, customization of software, systems integration, any implementation in the Participant's premises, audit certification or other legal process requested by the Participant, set-up fees, or enhancements. Fees for any such services that might be required for Participant and have been received shall be agreed separately and in advance between the Participant and IATA or its service providers.

8.3 Fees and charges are payable to IATA within thirty (30) days of billing. Fees and charges against members of the IATA Clearing House ("**ICH**") or the Airlines Clearing House ("**ACH**") shall be collected through the appropriate clearing house unless otherwise agreed. IATA may suspend provision of the Service upon thirty (30) days prior written notice in the event of failure by the Participant to settle any invoice or charge for the Service in a timely manner.

8.4 Any surplus revenues for the provision of the Service and the Additional Services will be reviewed by the SIS Steering Group, who shall have the right to propose an apportionment of the surplus to cover further development and/or a reduction in operating charges. IATA will use its best efforts to provide the Service at the lowest cost practicable.

8.5 The Parties recognize that the charges for the Service and/or Additional Services shall be calculated using a cost recovery model which is to balance over a one (1) year period unless an alternative period is agreed by the SIS Steering Group.

9. TAXES

9.1 Payment for fees and charges related to the use of the Service and/or Additional Services must be made by the Participant without any set-off or counter claim and free of deduction or withholding of any taxes or governmental charges (except as required by law). If any deduction or withholding is required by law, the Participant must pay the required amount to the relevant governmental authority, and pay to IATA as the case may be, in addition to the payment to which it is otherwise entitled under this Agreement, such additional amount as is necessary to ensure that the net amount actually received by IATA, free and clear of all taxes, equals the full amount IATA would have received had no such deduction or withholding been required.

9.2 Should any taxes, levies, charges or duties (including any goods and services or other value added tax) be imposed, levied or become payable on the supply of the Service and/or Additional Services made to Participant pursuant to this Agreement, the Participant shall pay any and all such taxes, levies, charges and duties, in addition to any other payments due under this Agreement. In the event IATA pays any such tax or assessment, Participant will immediately reimburse IATA upon demand. Notwithstanding the foregoing, neither Party shall be responsible for the other Party's taxes which are based on net or gross income or capital.

10. WARRANTIES AND LIABILITIES

10.1 The Participant hereby represents and warrants that:

10.1.1 it has obtained all operating licenses or government authorizations required for engaging in business;

10.1.2 it owns or has obtained all required rights in respect of any and all Data, including in relation to its collection, processing, provision, use, disclosure, validation and/or disposal as part of or in relation to this Agreement, the System, the SIS Solution, the Service or the Additional Services and all required rights otherwise necessary for the purposes of this Agreement, the whole in compliance with all applicable laws, including data privacy and data security laws;

10.1.3 it will use, handle, protect, dispose of and otherwise deal with any and all data of any and all other SIS Participants made available to it via the System and/or SIS Solution and/or otherwise by or through IATA solely for the purposes contemplated by this Agreement and in compliance with the terms and conditions of this Agreement and all applicable laws, and with a degree of care at least as high as the one that is applied to its own Data hereunder; and

10.1.4 it shall be responsible for ensuring that the Data or any attachment supplied by itself, its respective employees, agents, and contractors does not contain or introduce any Destructive Elements. If Participant becomes aware that a Destructive Element has been so introduced, Participant will eliminate the effects of the Destructive Element and, if the Destructive Element causes a loss (e.g., of operational efficiency or data), assist IATA to mitigate and restore such losses provided that it shall not prevent IATA from exercising any recourse it may have against Participant under this Agreement or at law. "**Destructive Elements**" means any software, data or tool (e.g., "viruses", "worms" or "trojan" programs) that (i) are intentionally designed to disrupt, disable, harm or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of the Service or related systems of IATA, including, for example, based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numeral (e.g., "time bombs", "time locks" or "drop dead" devices), (ii) would permit Participant or third parties to access the Service or related systems, to cause such disablement or impairment, or otherwise to circumvent the security features of the Service or related systems, or (iii) contain any other harmful, malicious or hidden procedures, routines or mechanisms which would cause the Service or related systems to cease functioning, or to damage or corrupt software, data or communications, or otherwise interfere with operations.

10.2 IATA hereby represents and warrants that:

10.2.1 it has obtained all operating licenses or government authorizations required to engage in its business;

10.2.2 it will use all commercially reasonable efforts to implement the Service. However, if IATA is unable, for any reason (including due to a Force Majeure Event), to implement the Service or similar Service or discontinues the Service or similar Service in accordance with this Agreement, IATA will have no further liability nor obligation to Participant other than to:

(a) mitigate the disruption to the interline settlement process;

(b) provide SIS Participants with continued access to the ICH and ACH (the latter being to the extent ACH authorizes IATA to provide such access) in accordance with the generally applicable terms of access to and use of the ICH and/or ACH, as the case may be; and

(c) propose an alternate service provider to provide the Service or similar Service and/or Additional Services in consultation with the SIS Steering Group, as further set out in Section 18.5.

The Steering Group may determine, upon IATA's consultation, that either option (b) or (c) is in particular circumstances not required, having taken due account of the operational requirements of the individual SIS Participants.

10.2.3 it will use all commercially reasonable efforts to perform or ensure that any of its subcontractors perform the Service and Additional Services and operate the System and SIS Solution in conformity to the Service Levels and Service Description as defined in Attachments D and E; in the event of any failure to meet such warranty, IATA shall promptly take corrective actions for future performance of such obligations in order to meet such warranty requirement;

10.2.4 it will use all commercially reasonable efforts to ensure that the Data supplied by the Participant and its respective employees, agents, and contractors, are promptly and accurately incorporated into the System, and made available for the purpose of the Service in accordance with the published calendars;

10.2.5 it shall be responsible for ensuring that any data and/or attachment supplied by itself, its respective employees, agents, and contractors for the purposes of performing the Service and/or Additional Services hereunder do not contain or introduce any Destructive Elements. If IATA becomes aware that a Destructive Element has been so introduced, IATA will eliminate the effects of the Destructive Element, and, if the Destructive Element causes a loss (e.g., of operational efficiency or data), assist Participant to mitigate and restore such losses, provided that it shall not prevent Participant from exercising any recourse it may have against IATA under this Agreement;

10.2.6 the performance of the Service and/or Additional Services under this Agreement and any related software which is used to provide, or which forms part of or is used in connection with the Service and/or applicable Additional Services, if any, do not and shall not infringe or misappropriate any intellectual property rights of a third party;

10.2.7 it will use, handle, protect, dispose of and otherwise deal with any and all data of Participant and other SIS Participants made available to IATA via the System and/or SIS Solution solely for the performance of the Service and Additional Services and other purposes as permitted by this Agreement, and in compliance with all applicable laws, including data privacy and data security laws, all of the foregoing being subject to Participant's representations and warranties in Sections 10.1.2 and 10.1.3 above; and

10.2.8 it has, and shall, at all relevant times, have the necessary rights to provide the Service and/or applicable Additional Services.

10.3 Notwithstanding any other provision of this Agreement to the contrary, each Party will be liable to the other Party for any actual direct damages incurred by the non-breaching Party as a result of the breaching Party's failure to perform its obligations in accordance with this Agreement, provided, however, that any and all liability and costs (including attorney's fees and legal expenses) incurred by IATA as a result of IATA's liability hereunder or inability to recover in whole or in part from Participant are subject to the cost recovery mechanism set out in Section 13.

10.4 EXCEPT FOR THE LIMITED EXPRESS WARRANTIES PROVIDED IN SECTION 10.2 ABOVE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IATA DISCLAIMS AND EXCLUDES ALL EXPRESS, IMPLIED, STATUTORY OR OTHER REPRESENTATIONS, WARRANTIES, AND CONDITIONS WHATSOEVER, INCLUDING THOSE PERTAINING TO TITLE, NON-INFRINGEMENT, SATISFACTORY CONDITION, MERCHANTABILITY AND FITNESS FOR PARTICULAR PURPOSE. IATA DOES NOT WARRANT THAT THE OPERATION OF THE SYSTEM AND THE SERVICE AND ADDITIONAL SERVICES WILL BE UNINTERRUPTED, AND/OR ERROR-FREE.

10.5 NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT TO THE CONTRARY AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR, AND EACH PARTY WAIVES AND RELEASES ANY CLAIMS AGAINST THE OTHER PARTY FOR, ANY CONSEQUENTIAL, SPECIAL, PUNITIVE, INDIRECT, OR INCIDENTAL DAMAGES RESULTING FROM PERFORMANCE OR FAILURE TO PERFORM UNDER THIS AGREEMENT, EVEN IF THE PARTIES KNEW OR SHOULD HAVE KNOWN OF THE EXISTENCE OR POSSIBILITY OF SUCH DAMAGES.

11. INDEMNIFICATION

11.1 The Participant shall indemnify and hold IATA, its directors, officers, employees and representatives, as well as the members of the SIS Steering Group and members of any other group of Participant representatives constituted to support the operation of the Service, harmless from any claim made by third parties (including other SIS Participants) in relation to any loss, prejudice or damage arising out of or in connection to this Agreement including acceptance, use, or distribution of the Data, or any subsequent use, distribution or loss of the Data by any party or person.

11.2 **Intellectual Property Indemnification**

11.2.1 IATA agrees to indemnify, defend and hold harmless Participant, its directors, officers, employees, representatives from and against all claims made by third parties (including other SIS Participants) as a result of any breach or inaccuracy of Section 10.2.6, provided that: (i) Participant provides IATA timely written notice of any applicable claim, (ii) Participant tenders the defense of any such claim to IATA for which IATA will thereafter select counsel and control the defense, (iii) Participant

may participate in such defense at its own cost, (iii) Participant will cooperate as needed in the defense of any such claim, and (iv) any and all costs relating to such indemnification are subject to the cost recovery mechanism set out in Section 13.

11.2.2 Without limiting the above, in the event of any such claim, IATA shall also, at its option, either:

(a) obtain the right to use the items or materials subject to such claim; or

(b) modify or replace such items or materials to become non-infringing.

11.2.3 Said IATA indemnification shall not extend to any liability which arises as a result of (i) use of such items or materials, Service and/or Additional Services in a manner inconsistent with instructions or documentation provided by IATA; (ii) combination of such items or materials, Service and/or Additional Services with software or other programs not provided by IATA, its subcontractors or agents.

12. VALIDATION OF DATA

12.1 IATA will not be responsible for nor have any liability to Participant for the content, correctness and validation of Data provided hereunder by the Participant or any third party acting on behalf of Participant, and Participant will indemnify and hold IATA, and its directors, officers, employees and agents harmless from and against any claim, loss, damage and costs (including reasonable legal and attorney's fees) suffered or incurred by IATA or its directors, officers employees and agents arising out of, or relating to, directly or indirectly, the content, correctness and validation of data transmitted by Participant or any third party acting on behalf of Participant hereunder or otherwise in connection with the Service and/or Additional Services.

12.2 Participant will, on a timely basis, inspect and review all reports submitted to it through the Service and/or Additional Services hereunder and will notify IATA of any errors therein no later than ninety (90) days following the receipt of such reports. Failure to notify IATA of any such errors within this period shall be deemed to constitute acceptance of such reports, but any errors may be reported at any time for the purpose of preventing similar errors in the future and enabling IATA to take appropriate action, if applicable.

13. COST RECOVERY

13.1 Given IATA's willingness to perform the Service and the Additional Services on cost recovery basis hereunder, Participant recognizes and agrees that IATA shall, at all times, be entitled to invoke cost recovery for any and all costs, liability, loss, prejudice and damage (including attorney's fees and legal expenses) incurred in connection to or arising out of the performance and operation of the Service and/or Additional Services, including costs, liability, loss, prejudice and damage in connection to or arising out of any (i) claims made by third parties as a result of IATA's performance or intended performance hereunder for, in relation to or for the intended benefit of Participant, or as a result of Participant's acts or omissions in connection to this Agreement, (ii) claims made by the Participant against IATA and (iii) claims made by IATA against any Participant, (altogether "**Claim(s)**"); provided, however, that such cost recovery shall be subject to the following process:

13.1.1 IATA shall provide prompt notice to the SIS Steering Group of any Claim or assertion of liability which could give rise to a loss that would be allocated to the Participants;

13.1.2 IATA shall advise and consult with the SIS Steering Group with respect to the defense of any such Claim;

13.1.3 If any loss or settlement of a Claim will result in recovery pursuant to the cost recovery of this Section 13, IATA shall provide to the affected SIS Participants prior written notice, for information purposes only, and include an explanation of the method of calculating the cost recovery allocation before taking action to recover such allocated amounts from the SIS Participant;

13.1.4 Any cost recovery allocation or calculation will be based on the relative utilization of the Service and/or Additional Services and in relation to the specific loss. The allocation methodology used by IATA will be subject to subsequent review by the Financial Committee upon request;

13.1.5 IATA will make all commercially reasonable efforts to mitigate losses, including by the use of disaster recovery services and the pursuit of insurance claims and other available recourse against third parties. Any such mitigation efforts shall be made in consultation with the SIS Steering Group;

13.1.6 IATA will communicate regularly with the SIS Steering Group with respect to the strategy, progress and costs of recovery efforts from third parties.

13.2 In the event that IATA invokes cost recovery from Participant and Participant pays its allocated share, thereafter, upon written request to IATA, Participant may be subrogated to any rights IATA may have had against any non-SIS Participant third party up to the amount actually paid, and IATA will cooperate in any efforts to independently assert such subrogated rights.

14. INTELLECTUAL PROPERTY RIGHTS

14.1 IATA or its licensors, suppliers or subcontractors shall have sole and exclusive ownership of all rights, titles and interests in and to the Service and/or Additional Services, including all intellectual property rights and any accompanying written or printed materials and copies thereof, and including all changes, derivations, modifications and enhancements thereto, including modifications pursuant to Section 6 hereof (together, the "**Materials**"). This Agreement does not provide Participant with title or ownership of the Materials, but only a right of limited access and use as described in Section 14.3.

14.2 Without limiting the foregoing, IATA is the owner of the SIS Solution and the System, and Participant is the owner of its Data.

14.3 IATA grants to Participant a limited right to access and use the System and the SIS Solution solely for the purposes of enabling Participant to obtain the benefit of the Service and applicable Additional Services during the Term of this Agreement and without further consideration to IATA. The foregoing right to access and use includes the right to permit contractors and other agents to access and use the System and the SIS Solution on Participant's behalf and the right to make and provide copies of user guides and other instructions to contractors and other agents, provided that such contractors and/or other agents have agreed that their access and use of the System and the SIS Solution and any user guides and instructions are subject to the same conditions and restrictions that apply to such access and use by Participant. It is agreed that any breach by such contractors and/or other agents of any such terms and conditions shall be deemed to be a breach by Participant of this Agreement and shall entitle IATA to pursue any and all remedies available to IATA.

14.4 During the Term of this Agreement, Participant grants IATA an irrevocable license to use, reuse, modify, create derivative works from and sublicense Data solely for the purpose or performing the Service and/or Additional Services hereunder.

14.5 IATA reserves the right to perpetually and irrevocably use and sublicense the Data in a Collated Data form (hereinafter further defined) solely for non-commercial purposes in promoting and reporting performance of the Service and/or Additional Services to present and prospective SIS Participants, including operational efficiency, training and international trending and benchmarking initiatives with respect to the Service and/or Additional Services. Any other use of Collated Data by IATA shall be agreed to in writing by the Participant in a separate agreement duly signed by Participant's and IATA's respective authorized representatives. For the purpose of this Agreement "**Collated Data**" means a set of de-identified and aggregated Data collated by IATA from the Participant and other SIS Participants in the Service, which contains no names or information that would, in any way, allow identification of the Data of Participant or any other individual SIS Participant.

14.6 The terms and conditions set forth in this Section 14 shall survive termination or expiry of this Agreement.

15. CONFIDENTIALITY

15.1 Each Party may be given access to information (verbally or in hardcopy and/or electronic form) that relates to the other Party's past, present, and future research, development, business activities, products, services, and technical knowledge, which is identified by the discloser as confidential or

would be treated as confidential by a reasonable person given the nature of the information or the circumstances surrounding its disclosure or access ("**Confidential Information**"). Notwithstanding the foregoing, Confidential Information will not include any information which (i) is at the time of its disclosure publicly known or within the public domain without recipient's breach of this Agreement (ii) is, prior to its initial disclosure hereunder, in the possession of the disclosing Party as evidenced in a documentary form and was not the subject of an earlier confidential relationship with the other Party; (iii) is independently developed by the disclosing Party without use of or reference to any of the other Party's Confidential Information; or (iv) is acquired by the disclosing Party from any third party having a right to disclose it to the receiving party. Each Party may disclose Confidential Information to the extent required by a court of competent jurisdiction or other governmental authority or otherwise as required by law, provided that the disclosing Party will, to the extent permitted pursuant to such disclosure order or law, use commercially reasonable efforts to notify the other Party in advance of such disclosure so as to permit such Party to request confidential treatment or a protective order prior to such disclosure.

15.2 Each Party shall keep confidential, and shall not disclose to any third party for any reason, any Confidential Information of the disclosing Party without the prior written consent of the disclosing Party at its sole discretion, except to (i) its respective employees, agents and contractors on a need to know basis and (ii) in case of IATA, to its service providers that are directly responsible for operating and managing the Service and/or Additional Services, but only to the extent necessary for purposes of this Agreement provided that such service providers are bound by same or substantially similar terms and conditions than those contained in this Section 15. Furthermore, IATA may use or make copies of the Confidential Information of the Participant only to the extent necessary for purposes of this Agreement.

15.3 Subject to this Section 15, IATA reserves the right to use the Data for purposes of allowing IATA to perform the Service and/or Additional Services.

15.4 The terms and conditions set forth in this Section 15 shall survive termination or expiry of this Agreement.

16. MONITORING

IATA may monitor individual use of and access to the Service to ensure compliance with the rules, policies, deadlines and instructions applicable thereto. The Participant using the Service expressly consents to such monitoring. If such monitoring reveals possible criminal activity or unauthorized use, IATA may immediately suspend the individual user's access and/or the Participant's access to the Service and/or provide the evidence of such monitoring to law enforcement officials. IATA shall notify the Participant of any such action to be taken unless instructed otherwise by the law enforcement officials. IATA reserves the right to maintain and, for any legitimate reason, review logs containing any inquiry details and other activities performed by the Participant in connection with the Participant's use of the Service. Participants will be notified if any potential fraud or breach of security is identified.

17. PUBLICATION

All notices and documents to be issued under this Agreement shall be issued by IATA and distributed to all interested parties.

18. TERM AND TERMINATION

18.1 This Agreement shall commence on the Effective Date and, subject to paragraph 18.2, shall continue for an initial term of one (1) year, and thereafter shall automatically renew for successive periods of twelve (12) months each (the "**Term**").

18.2 Either Party may terminate this Agreement by giving the other not less than six (6) months written notice, which notice shall be given in accordance with Section 22. However, no such notice of termination may become effective before the expiration of twelve (12) months from the Effective Date. The Steering Group may agree to reduce or waive any of the notice requirements set out in this Section 18.2.

18.3 In the event of a termination of this Agreement by IATA in accordance with Section 18.2, IATA, at the Participant's request, will provide mutually agreed upon transition services for a period of at least ninety (90) days from the effective date of the termination or any other mutually agreed to period of time to allow the Participant to find and retain alternative application and service providers.

18.4 During the Term of this Agreement, in the event of a material breach, the non-breaching Party may terminate the Agreement, in whole or in part, by giving thirty (30) days written notice to the breaching Party specifically identifying the breach, unless the breach is cured by the breaching Party within the thirty (30) day period. Material breach by Participant includes when Participant is in default of payment of fees and charges for Service and/or Additional Services as per Section 8.3 for more than sixty (60) days (unless such fees and charges are subject to a legitimate dispute between the Parties acting in good faith). For sake of clarity, IATA's acceptance of the indemnification under Section 11.2 shall constitute a cure for the purposes of this Section 18.4. Either Party may also terminate this Agreement on written notice to the other Party (i) if an Event of Insolvency occurs with respect to the other Party, or (ii) as otherwise expressly allowed hereunder. A Party affected by an Event of Insolvency in respect of itself must immediately notify the other Party in writing of the occurrence of such Event of Insolvency. "**Event of Insolvency**" means any instance where a Party makes a general assignment for the benefit of creditors, or files a voluntary petition in bankruptcy or petitions for reorganization or arrangement, or where a petition in bankruptcy is filed against a Party, or where a receiver or trustee is appointed for all or any part of the property and asset of a Party, or otherwise commit any act of insolvency, under any Laws of New York and of any other jurisdiction in the world relating to bankruptcy, insolvency, stay of creditor remedies, moratorium, compromise, arrangement, extension, adjustment or reorganization of debts or other liabilities, liquidation, winding-up or dissolution, excluding any solvent reorganization or scheme arrangement.

18.5 **Withdrawal from providing the Service and Additional Services**

18.5.1 In the event IATA, for any reason (including due to a Force Majeure Event), completely withdraws from providing the Service and Additional Services, and does not offer any comparable service providing similar functionalities, IATA agrees to transfer to an alternate service provider necessary license(s) and related intellectual property to provide the Service and Additional Services, subject to a commercially reasonable process intended for IATA to recover all investment costs put in the SIS Project, including cost of capital, which process shall be at IATA's discretion.

19. INSURANCE

19.1 IATA hereunder shall, during the Term of this Agreement (as regards insurance on an event-occurring basis) and for at least 6 years after expiry or termination of the Agreement for insurance on a claims made basis, maintain at its own cost the following insurance coverage:

19.1.1 Commercial general liability insurance for bodily injury and property damage in an amount not less than US$2 million each occurrence; and

19.1.2 Professional and Technology Liability/Errors and Omissions, including professional liability, technology products, employee fraud/dishonesty and computer fraud insurance in an amount not less than US$5 million.

19.2 In the event that the insurance coverage is to be cancelled or materially changed, IATA shall give Participant at least thirty (30) calendar days prior written notice.

19.3 IATA shall provide Participant with a certificate of insurance in customary form evidencing such coverage upon request.

20. FORCE MAJEURE

Neither IATA nor Participant shall be liable for any default, delay or failure to provide the Service and/or Additional Services under this Agreement caused directly or indirectly from any cause beyond IATA's or Participant's reasonable control including, acts of God, acts of governmental agencies, acts of war, riots, fires, freight embargoes, severe weather, floods, earthquakes, natural disasters, explosions or other catastrophes ("**Force Majeure Event**"). Delays by suppliers or

vendors are not considered Force Majeure Events, unless those suppliers or vendors themselves are prevented from delivering the service or otherwise performing their obligations due to a Force Majeure Event. Notwithstanding the above, IATA shall make all reasonable efforts to restore the Service and/or Additional Services as promptly as possible.

21. ASSIGNMENT

Neither Party may assign its respective rights and/or obligations under this Agreement without the prior written consent of the other subject to the following exceptions: (a) if the Participant wishes to assign its rights or obligations IATA's consent shall not be unreasonably withheld or delayed; and (b) IATA may assign this Agreement to a successor entity that is a not for profit trade association performing substantially the same functions as IATA, effective on notice to Participant but without needing Participant's prior written consent.

22. NOTICE

Any notice to be served under this Agreement shall be in writing and sent either by first class post, by facsimile or e-mail, to the following address of each Party and in such case will be deemed to be received upon the earlier of actual receipt or two (2) working days after sending.

Name:
Address:
Attn:

IATA:

International Air Transport Association
800 Place Victoria, P.O. Box 113
Montréal, Québec
Canada
H4Z 1M1

Attn: GDC Particpation (www.iata.org/cs)

23. GOVERNING LAW AND DISPUTE RESOLUTION

23.1 Laws

This Agreement shall be governed by and construed in accordance with the laws of the State of New York, United States of America, without regards to any conflict of law provisions. To the extent applicable, the Parties expressly agree to exclude the application of the U.N. Convention on Contracts for the International Sale of Goods (1980) to this Agreement.

23.2 Dispute Resolution

23.2.1 Amicable Resolution

The Parties shall attempt to amicably resolve any dispute, controversy or claim relating directly or indirectly to, or arising out of, or in connection with, this Agreement (the "**Dispute**"). In the event the Parties have failed to resolve such Dispute within twenty (20) calendar days after receipt of a notice, then the Parties shall refer such Dispute for settlement to their respective officers who shall make every effort to reach an agreement on such Dispute. In the event the Parties' respective officers fail to resolve such Dispute within fifteen (15) calendar days, either Party may, without further notice, submit such Dispute to arbitration in accordance with Section 23.2.2.

23.2.2 Arbitration

If the Parties fail to amicably settle a Dispute in accordance with Section 23.2.1 above, either Party may, without further notice, submit the Dispute to arbitration. The Parties agree that such Dispute shall be exclusively and finally settled by arbitration conducted in accordance with the Rules of Arbitration of the International Chamber of Commerce (the "**Rules**") in effect on the date of notification of arbitration hereunder submitted in accordance with the Rules, or such other procedures as the parties may agree in writing. The Parties agree to permit an ICC arbitration panel to grant preliminary or permanent relief available pursuant to the Rules and New York law. The arbitration shall take place in Montreal (Quebec, Canada) and the language for the proceedings shall be English. The arbitral tribunal will be composed of three (3) arbitrators appointed in accordance with the Rules. The arbitration award shall be final and binding upon the Parties, the Parties renouncing to appeal against the arbitration award by any ordinary or extraordinary means. The arbitration award may be enforced by action before any court of competent jurisdiction. The Parties shall treat as confidential the arbitration, the content of the proceedings, the terms of any order or award and any documentary or other evidence disclosed during the arbitration. Service of any request for arbitration made pursuant to this Section must be made in accordance with the Notice provisions in Section 22.

23.2.3 Arbitration–Joining Disputes

If any dispute arising out of or relating to this agreement (hereinafter referred to as a "**Related Dispute**") raises issues which are substantially the same as or connected with issues raised in another dispute which has already been referred to arbitration by another signatory to the IATA standard agreement for SIS participation (an "**Existing Dispute**"), the tribunal appointed or to be appointed in respect of any such Existing Disputes shall also be appointed as the tribunal in respect of any such Related Dispute, if:

(a) the request for arbitration in the Related Dispute is submitted, in accordance with Clause 23.2.1, prior to the terms of reference of the Existing Dispute being signed or approved in the Existing Dispute in accordance with Article 18(2) or 18(3) of the Rules; or

(b) the parties to both the Existing Dispute and the Related Dispute agree to the disputes being heard together.

Where, pursuant to the foregoing provisions, the same tribunal has been appointed in relation to two or more disputes (i.e. an Existing Dispute and a Related Dispute), the tribunal shall order that the whole or part of the matters at issue shall be heard together upon such terms or conditions as the tribunal thinks fit. The appointment of arbitrators where there are multiple parties to the arbitration shall be in accordance with Article 10 of the Rules.

24. NATURE OF THIS AGREEMENT

This Agreement shall be solely for the benefit of, and shall be enforceable only by, the Parties and their respective successors and permitted assigns, and no other person or entity is or shall be entitled to bring any action to enforce any provision of this Agreement against either Party.

25. COUNTERPARTS

This Agreement may be signed in any number of counterparts. Each signatory shall hold one counterpart.

26. SEVERABILITY

The invalidity, illegality or unenforceability of the whole or part of any clause or term or condition does not affect or impair the continuation in full force and effect of the remainder of this Agreement.

27. USE OF SYMBOL & LOGOS

Except as otherwise provided in this Agreement, the Parties shall not use, display or reproduce the symbols or logos of each other in any way without the prior written permission of the other Party. Without limiting the foregoing, any proposed use of the name or logo of each Party must be submitted to the appropriate Party's corporate secretary division for prior written approval. Notwithstanding the above, the Participant shall be deemed having given its consent to IATA, for the purposes of providing the Service or Additional Services, to use, display or reproduce its logo and/or symbol by loading them into the System.

28. SURVIVAL

Notwithstanding any termination of this Agreement, either Party's rights and obligations under Sections 10 (“Warranty”), 11 (“Indemnification”), 13 (“Cost Recovery”), 14 (“Intellectual Property Rights”), 15 (“Confidentiality”), 18.3, 18.5, 19 (Insurance”), 23 (“Governing Law and Dispute Resolution”), Attachment G (Data Security Agreement) where applicable and any other Sections or clauses which by their nature should survive termination of this Agreement, shall survive any such termination.

29. LANGUAGE

The Participant and IATA have mutually agreed to draft the Agreement in the English language. *Les parties acceptent que la présente entente, ainsi que tout avis ou document y afférent, soient rédigés en langue anglaise.*

Done this _____ day of _____ 20_____

For the International Air Transport Association

Signature:_____

Name: Adina Minculescu_____

Position: Head, e-Invoicing Services, GDC_____

Date:_____

For the Participant

Signature:_____

Name:_____

Position:_____

Date:_____

For the Participant

Signature:_____

Name:_____

Position:_____

Date:_____

ATTACHMENT A—PRICING SCHEDULE

The Service will be run on an operational cost-recovery basis, and the fees are subject to adjustment to ensure that operational costs are recovered. The prices below are effective 01 January 2019 and reflect the current best estimate of the charges necessary to operate the SIS Solution on a cost-recovery basis. As more information is made available to IATA about the estimated and actual use of the Service, prices will be adjusted in order to maintain neutral revenue. The annual accounts of the SIS operations covering the actual and planned cost and revenues will be shared with the SG in a timely manner.

1. BASIS OF CHARGING–ANNUAL SIS FLAT FEE

The SIS Annual Fee will be charged to every SIS participant from the date of signature of the agreement at the following rates:

Band	Invoices Submitted Annually From	To	IATA Member Airlines	Non-IATA Member Airlines, Airline Subsidiaries, ICH Sponsored Airline Members	IATA Strategic Partners, Other Sponsored or Subsidiary Participants	Associate Members, Other Participants
1	0	799	$1,000	$2,250	$3,250	$4,500
2	800	7,999	$2,500	$4,000	$5,000	$6,500
3	8,000	15,999	$4,000	$6,500	$7,500	$9,000
4	16,000	24,999	$5,500	$8,500	$9,500	$11,000
5	25,000		$7,000	$10,000	$11,000	$14,000

The charging band for new ICH or ACH participants will be Band 1, re-assessed quarterly on an annualised volume basis until twelve months history is available.

In all other cases, the charges will be re-assessed on an annualised basis each quarter and adjusted in arrears if the annualised total (or prorated equivalent) has exceeded or fallen below the threshold used.

2. BASIS OF CHARGING–SIS TRANSACTION FEES

When using the Service, transaction fees will be charged for each submission of a transaction or record by the billing participant or its agent. The amount paid per transaction depends upon the total Service transaction fees paid by the Participant in the previous quarter and will fall into one of the following categories:

SIS Transaction Fee Ranges	
From	**To**
$0	$4,999
$5,000	$14,999
$15,000	

After determining the proper category in the chart above, the following chart will be used to determine the actual transaction prices to be charged:

	SIS Transaction Fees		
Quarterly volume threshold	**$0–$4,999**	**$5,000–$14,999**	**$15,000 +**
Transaction Type	**(base)**		
Invoices–per *Pax, Cargo, UATP, Misc*	$0.57	$0.45	$0.33
△ **Group A1–per** *Pax:* Prime Coupon, Credit Memo, Sampling Provisional Invoice Coupon, Sampling Digit Evaluation Coupon, Value Determination Request, Auto-billing Request[1]	$0.0074	$0.0059	$0.0043
Cargo: Original Billing (AWB), Credit Memo			
Group A2–per *Pax:* Billing Memo	$0.0171	$0.0135	$0.0099
Cargo: Billing Memo			
Group B1–per *Pax:* Sampling UAF Coupon	$0.0114	$0.0090	$0.0066
Group B2–per *Pax:* Rejection Memo (including Sampling), Correspondence *Cargo:* Rejection Memo, Correspondence *Misc:* Correspondence	$0.0342	$0.0270	$0.0198
Supporting Documents–per kilobyte *Pax, Cargo*	$0.0011	$0.0009	$0.0007
Misc	$0.0016	$0.0014	$0.0012
Digital Signature (& Validation, as appropriate)	$0.15	$0.15	$0.15
Optional legal archiving (per invoice)	$0.10	$0.10	$0.10

* All transactions entered via the IS-WEB interface and not via IS-IDEC or IS-XML (including Correspondence, which are only entered via IS-WEB) will be charged an additional 25%. This surcharge will not apply to supporting documents uploaded via the IS-WEB interface.

Additional Notes on the Service Transaction Fees:

- For the purposes of determining the proper category, fees will only take into account the Service transactional charges and not any annual fee paid.
- Digital signature charges may be payable by both the billing and billed Participant based on their selections.
- Supporting Document charges are based on the stored document size (documents are stored unzipped), not the transmitted document size (documents are transmitted zipped).
- Where twelve months of data is not available, the Base charging band will be applied, and re-assessed quarterly on an annualised volume basis until twelve months history is available.
- **Effective January 2018** - Rejection Memo, Billing Memo and Credit Memo charges are based on the count of memo coupon/AWB breakdowns instead of RM/BM/CM memo counts.
- A&A fees are **not** included in the above figures and will be charged separately by A&A. The “Value Determination” and “Auto-billing” features of Integrated Settlement require the storage option from A&A.

[1] The charge for auto-billing request does not include the invoice and prime coupons that are then submitted on the carrier's behalf; those are charged additionally at the described rates.

3. OTHER CHARGES

3.1 Access to the general file testing system (the “sandbox”) will be provided free of charge at all times.

3.2 Support will be charged at USD500 per day for any technical support required during the Sandbox or certification testing process.

☐ 3.3 Access to the multi-account optional feature* will be charged as per the below:

No. of Additional Accounts	Annual Fee (x account/year)	Minimum Fee	Maximum Fee
Between 2–4	$500	$1,000	$2,000
Between 5–12	$400	$2,000	$4,800
More than 12	$5,000 flat fee	n/a	n/a

☐ *The multi-account functionality allows SIS users of group companies, subsidiaries or merged entities to access multiple SIS member accounts using a single email address. For more information about this feature contact us via the IATA Customer Portal at www.iata.org.cs.

ATTACHMENT B—SERVICE AND ADDITIONAL SERVICE OPTIONS

1. PURPOSE

1.1 This attachment describes the Additional Services that the Participant elects to use in addition to the provision of the Service under the main agreement. This annex may be amended at any time by the Participant and communicated to IATA in order to reflect the changes in its selection of Additional Services.

2. GLOSSARY

See Glossary in Attachment D “Service Description”.

3. OPTIONAL SERVICES

3.1 Digital Signature application

SIS offers a digital signature (DS) application service in a number of countries with the help of a trusted digital signature service provider. Based on the instructions provided by the billing entity, SIS creates an invoice subset file from the SIS-format invoice data with the necessary legal and invoice information fields. This digitally signed file is made available by SIS as one of the outputs to the billing entity at the end of the billing period, based on the configuration of the Member Profile. It can also be downloaded online over the IS-WEB.

SIS allows billed entities to configure the application of Digital Signature on Payable Invoices in the Member Profile. Based on the location details specified on the payable invoice, SIS triggers the process to apply digital signature in the countries covered by the service.

3.2 Digital Signature verification

SIS provides an option whereby the billed entity can request verification of the digital signature applied on Payable Invoices, via the Member Profile. A verification log file is created by this process which contains the status of the applied digital signature in the countries covered by the service.

3.3 Legal Archiving (or E-Archiving) service

Some jurisdictions may require legal storage for the digitally signed invoices for varying amounts of time. During this period, the invoices and any applicable digital signature need to be accessible for any audits. To address this issue, SIS will provide an optional Legal Archiving service to store the digitally signed invoices and other related information on behalf of the Participant in an external Legal archive for a longer period as required by the local regulations.

3.4 Billing Value Determination

As part of this service, SIS accepts Usage Files (modified Record 50 file format as defined in the SIS Participation guide) from billing entities requesting prorate values for coupons utilized by them. SIS validates the file format and forwards the Usage File to ATPCO for further processing. The processed information is provided by ATPCO back to SIS. SIS forwards the output files provided by ATPCO to the billing entities.

3.5 Billing Value Confirmation

SIS generates a Billing Value Confirmation file for passenger prime billing coupons where both the billing entity and billed entity are subscribers to this service. This file is forwarded to ATPCO for further processing. ATPCO validates the billing values with the prorate values stored within its database. Any exchange rate conversions of the prorate values as per the billing month will be done by ATPCO before comparing the values. The results of the comparison are updated by ATPCO and provided to SIS. SIS updates the comparison results within its Billing Record Database.

3.6 Auto-billing

As part of this service, SIS will store the prorate records received through the Value Determination process and generate invoices on behalf of the Billing Entity. On a daily basis SIS will generate a Revenue Recognition File (File Format defined in the SIS Participation Guide) containing the billing records of coupons included in the Auto-Billing Invoices.

The Auto-Billed invoices are automatically closed and finalized by SIS and processed further like any other IS-IDEC/IS-XML invoices. At the end of the billing period, SIS generates an Invoice Posting File which includes details of all Auto-Billed invoices

3.7 Summary table of Optional Services selected

By indicating that the Optional Service is "ON" in the below table, the Participant hereby confirms that IATA is to provide this additional service and that the fees described in Attachment A of this agreement applicable to the Optional Services selected will be charged to the Participant.

Optional Service	ON/OFF
Digital Signature application	ON ☐ OFF ☐
Digital Signature verification	ON ☐ OFF ☐
Legal Archiving	ON ☐ OFF ☐

Applicable to A&A Members only	ON/OFF
Billing Value Determination	ON ☐ OFF ☐
Billing Value Confirmation	ON ☐ OFF ☐
Auto-billing	ON ☐ OFF ☐

For the Participant

Signature:_____

Name:_____

Position:_____

Company:_____

ATTACHMENT C—GOVERNANCE

1. SIS STEERING GROUP

1.1 Role/Mandate

△ The SIS Steering Group shall act as advisor to the Financial Committee, other relevant IATA bodies, and IATA Management, on matters related to the Simplified Invoicing and Settlement (SIS) product.

Areas of activities include:

(a) Maintaining global oversight of the ongoing SIS operation and development to ensure that SIS provides cost effective, high quality settlement services that are relevant to IATA members' needs.

(b) Providing a consultative forum between IATA management and Member airlines on the efficient operation of the service.

△ (c) Advising IATA management on prioritisation of developments and changes to functionalities of the Simplified Invoicing and Settlement System as proposed by the user communities or the service providers and supporting any system testing as requested by IATA.

(d) Providing guidance to IATA management in respect of the pricing policies for the operation of the service.

(e) Reviewing any audit risk and risk issues associated with the service.

(f) Proposing changes to electronic invoicing processes and standards, in particular management of the IS-IDEC and IS-XML standard for electronic invoicing, determination of e-invoicing formats, submission methods, electronic documentation requirements, and changes to mandatory fields.

(g) Reviewing proposed changes in billing rules or transaction processes arising from Industry meetings and consider their implications on service delivery.

(h) Drafting and proposing any changes that may be required to the IATA Revenue Accounting Manual after considering inputs from SIS participants.

(i) Coordinating with other IATA Industry e-invoicing Services with regards to interfaces between the services.

(j) Coordinating with the XML Working Group wherever a common approach to standards may benefit the industry.

1.2 Membership

1.2.1 The SIS Steering Group consists of the following members:

(a) IATA's Director for Financial and Distribution Services Operations

(b) IATA's Manager, Airline Distribution Standards (Pay/Account Vertical)

(c) Secretary/Treasurer of the Airlines Clearing House

(d) Chair of the ATA Revenue Accounting Committee

(e) Chair of the Interline Billing & Settlement Operations Working Group

(f) 5 members appointed by the Financial Committee based on the results of the election at the SIS General Meeting

(g) Up to 5 additional members appointed by the Financial Committee based on members nomination

1.2.2 The members appointed by the Financial Committee shall be qualified representatives within IATA member airlines who have knowledge and experience of the operations of the interline billing and settlement process.

1.2.3 No more than one person associated with or employed by the same airline may be a representative on the SIS Steering Group at any one time.

1.2.4 The appointments shall take into consideration:

(a) Industry expertise

(b) Potential contribution to the Working Group's work

(c) Seniority within the airline of the candidate concerned

(d) Regional balance

(e) Airline alliance balance (including non-alliance airlines)

(f) Candidates from airlines that share a common ownership structure

(g) Size of Member airline balance

(h) A combination of continuity and rotation in the Working Group membership

(i) Representation of the membership across all of the Working Groups

(j) Feedback from the Industry

△ 1.2.5 Each Member shall be appointed for a term of up to three years, which can be renewed up to a maximum of two times. If a person has served three consecutive terms, a minimum of two years must expire before that person is eligible again for appointment to the same Working Group. The Financial Committee may exceptionally approve the appointment of a person to serve more than three consecutive terms on the basis of his or her knowledge and experience.

1.2.6 Members may not appoint a proxy to represent him or her.

1.2.7 Each Member shall act as a representative of the membership as a whole and not as a representative of his or her region or of the Member that nominated him or her.

△ 1.2.8 The SIS Steering Group shall elect a Chair and Vice-Chair whose terms shall be for three years, with an expected rotation after 2 terms, through a simple majority vote.

1.2.9 The Chair and Vice-Chair shall operate as a full member of the SIS Steering Group.

1.2.10 IATA will appoint a secretary to work with the SIS Steering Group and coordinate its activities within IATA.

1.2.11 Membership shall terminate if:

(a) The airline ceases to be a Member, or

(b) The Member leaves the relevant position in the airline, or

(c) The Member fails to attend two consecutive meetings, or

(d) The Member fails to attend 2 consecutive conference calls in a given calendar year.

1.3 Meetings and Procedures

1.3.1 The SIS Steering Group shall meet as required, including by teleconference, video conference, or other electronic means. It shall meet in person at least twice per year. It shall normally meet within six to eight weeks prior to the Financial Committee meetings to enable reporting to the Financial Committee.

1.3.2 Meetings shall be called by IATA, in consultation with the Chair.

1.3.3 IATA shall normally give thirty days' notice of the meeting; at least ten days' notice shall be given for a special meeting.

1.3.4 A simple majority of the SIS Steering Group members shall constitute a quorum for any meeting.

1.3.5 Attendance at meetings will be limited to Group Members. A limited number of qualified observers may be invited to attend specific meetings at the invitation of IATA. Where their knowledge or advice would be useful in attaining the objectives of the meeting, representatives of relevant international organisations and regional airline associations may be invited by IATA to attend meetings as observers.

1.3.6 The agenda of any meeting shall include any relevant matter proposed by:

(a) Any member of the Group

(b) IATA

(c) The Financial Committee or one of its Working Groups

(d) Any SIS participant whose representative shall be entitled to attend the SIS Steering Group meeting

1.3.7 The SIS Steering Group will seek to operate on a consensus basis, based on members present.

1.3.8 The SIS Steering Group may establish its working procedures consistent with these Rules.

1.3.9 Subject to the Financial Committee's approval, the SIS Steering Group may request the creation of a technical Task Force to address a specific technical issue. The Task Force terms of references shall state its specific objectives, work programme, deliverables, agreed timetable, and membership. Such Task Force will be reconfirmed by the Financial Committee annually and be disbanded once its mandate has been completed.

1.3.10 These terms of reference, including the quorum may be amended from time to time by IATA's Director General or the Financial Committee.

1.3.11 The work of the SIS Steering Group shall be conducted in full compliance with applicable competition and antitrust law, with supervision from IATA Legal Counsel.

1.4 Work Programme

1.4.1 The SIS Steering Group shall develop an annual Work Programme which will be reported as part of the overall subject activity to the Financial Committee. The report will be developed on a consensus basis.

2. SIS OPERATIONS:

2.1 SIS Operations is the IATA unit responsible for the management and delivery of the Service. It will be managed in accordance with IATA policies and will be responsible for the following:

(a) Managing the operations and development of the services, delivery and systems needed to deliver the Service.

(b) Managing the development and delivery of the enhancements to the Service.

(c) Interpretation of the SIS Steering Group user requirements into Functional and Technical Specifications assisted by any Technical Task Force where relevant.

(d) Obtaining input on the finalised Functional and Technical Specifications from any Technical Task Force and Participants.

(e) Obtaining support for the specifications from the SIS Steering Group.

(f) Providing cost estimates for the functional and technical specifications generated by the SIS Steering Group in a timely manner and obtaining sign-off for development from IATA as appropriate.

(g) Development of appropriate business cases/models based on Airline/industry benefits.

(h) Development of pricing proposals for product enhancements seeking support from the SIS Steering Group.

(i) Prioritising resource allocation in line with delivery priorities agreed with the SIS Steering Group.

(j) Working with their technical teams to manage the development efforts necessary to deliver the required functional and technical specifications.

ATTACHMENT D—SIMPLIFIED INVOICING AND SETTLEMENT (SIS)—SERVICE DESCRIPTION

Simplified Invoicing and Settlement (SIS) Service Description

1. BACKGROUND

The SIS project aims to simplify interline billing, and to remove paper from the entire process, delivering tangible financial benefits to the industry. The vision is that a billing entity will submit a single electronic billing file that will be converted into an invoice and a settlement file, sent to the billed entity, and cleared through the relevant clearing house. As part of this project, an "Simplified Invoicing and Settlement (SIS) System has been developed based on the principles of completely paperless billing, invoicing, and settlement. The SIS solution encompasses Passenger, Cargo, Miscellaneous and UATP interline billings with settlements through ICH, ACH or on a bilateral basis.

In this document the terms Simplified Invoicing and Settlement (SIS) and Integrated Settlement (IS) may be used interchangeably and the term SIS Member(s) has the same meaning as Participant and/or SIS Participants, as the case may be.

1.1 Overview of Simplified Invoicing and Settlement (SIS)

SIS is an Invoicing Platform which is connected to various external systems such as ICH, ACH, ATPCO, a trusted Digital Signature service provider, etc, thus providing a single point of communication for Interline billing, invoicing and settlement.

A high level overview of SIS is shown in Figure 1 below:

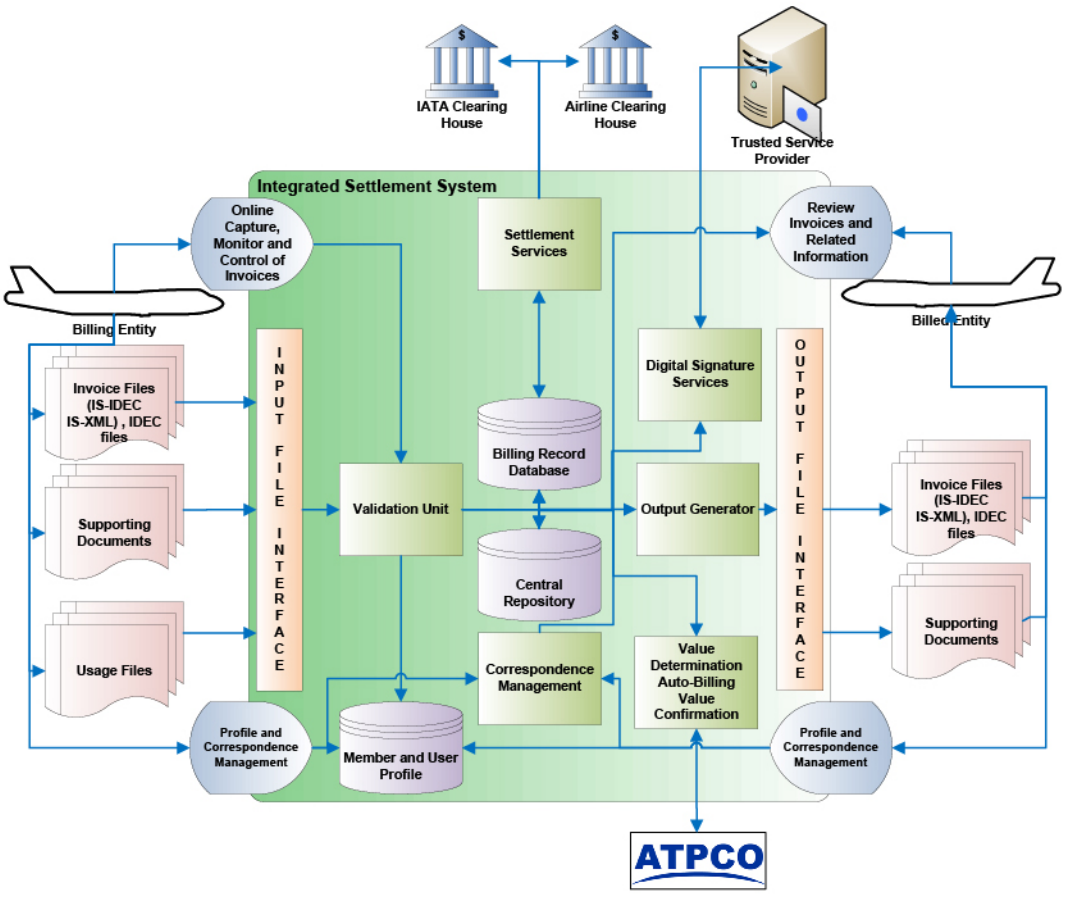

Figure: Overview of Simplified Invoicing and Settlement (SIS)

The SIS application can be grouped into the following logical modules:

- SIS Member and User Management
- Receivables Data Processing
- Payables Data Processing
- Correspondence Management

The services provided by each module are described in the subsequent chapters.

1.2 Supporting Documentation

The following documents provide additional information to the services described in this document:

- *SIS Participation Guide:* This document provides the details of the impact of SIS on the IT systems and processes of the SIS Members.
- *Sign up and Certification Guide:* This document provides detail explanation on the Sign up process and steps to be followed to get certified for SIS.
- *IATA Revenue Accounting Manual (RAM):* The RAM contains all the rules and procedures associated with interline billing, with which the SIS application will be compliant, and of which the SIS Participation Agreement and this Attachment are a part.
- *ACH Manual of Procedure:* For members of the ACH, the Manual of Procedure contains all the rules and procedures associated with billings using the ACH for settlement.
- *SIS User Guide:* This manual documents all the functional processes of SIS that are available to the individual user.

1.3 Standard Services and Optional Services

Standard Services such as submission of invoices, flight coupon data, air waybill data, rejections etc are available to any Member as soon as participation formalities have been completed. Optional Services require specific notification or request to SIS Operations (SIS-Ops), whether before or after use of the service has commenced. Use of optional services will incur additional charges (such as Digital Signatures) and may also require secondary agreements to be signed (such as for A&A services). Because a service is shown as 'Optional' in SIS does not mean that it is optional in the Members operating jurisdictions.

2. MEMBER AND USER MANAGEMENT

The SIS application allows SIS Members to configure their company and staff responsibility details using the Member Profile module over IS-WEB.

2.1 Member Creation

The initial set-up of SIS Member is done by SIS-Ops using existing information within IATA, ICH, ACH etc as well as using information sourced from individual members during the sign-up process. This is done for all airline entities defined in the Airline Coding Database as well as non-airline entities who are members of ICH and/or ACH. Once the participation formalities are completed, the Membership status is activated by SIS-Ops and a Super user account is created and provided to the SIS Member. Login credentials to access IS-WEB as well as the FTP server (if required) are also provided by SIS-Ops so that the SIS Member can communicate with the SIS Platform.

Note: *The SIS Member will have to go through the Sandbox Testing and Certification process to be able to send invoice files to SIS. This process is described in detail in the SIS Sign Up and Certification Guide.*

2.2 Member Profile Set-up

Using the login credentials provided by SIS-Ops, the SIS Member can login to IS-Web and review the set-up details on the Member Profile Screen. SIS allows the SIS Member to update the details on the Member Profile. Certain fields on the Member Profile will only allow changes to be made which will be applicable for a future billing period or date.

Member Details

SIS application will allow the SIS Member to upload and store its official logo on to its platform. This logo will be used by SIS to display the image on the PDF invoices generated on behalf of the SIS Member. The Member's Accounting Code, Prefix, Legal Name, Status in SIS, IATA, the ICH, or the ACH, and the details of the Member's bank accounts for bilateral settlements cannot be changed by the SIS Member and must be referred to SIS-Ops.

Location Details

Every SIS Member needs to have at least one location detail setup in the Member Profile. This will be the default location of the SIS Member and is referred to as the “MAIN” location. The SIS Member will be allowed to update the details of the MAIN location as well as create any additional location details that may be required for legal or business reasons. This information is used at the time of PDF Invoice generation as well as when generating the Payable output invoices, in case the invoice reference data is not provided in the incoming receivables invoice.

Bank Details for Bilateral Settlement

Bank details can be set-up against each location created in the Member Profile to be used in case of bilateral settlement invoices. This set-up can only be done by SIS-Ops based on signed physical requests from the SIS Members. This information is included by SIS in the Payable Invoice in case of Bilateral Settlement.

Contacts

SIS allows set-up of two types of contacts in the Member Profile:

- *Informational Contacts:* These contacts are set up for purely informational purposes, For example Passenger RA Manager, etc. The contact details include information such as the name, designation, address, contact numbers, email id etc of that person. The SIS application allows SIS Members to retrieve the informational contacts of other SIS Members. As part of the initial data set-up, SIS-Ops will configure some of the informational contacts of the SIS Member based on the data available within IATA (RAM, ACH Manual of Procedure, ICH database, etc).
- *Processing Contacts:* These contacts, if set up by the SIS Member, will receive email alerts on specific events related to invoice processing e.g. Passenger File Receipt Alert Contact, Cargo Correspondence Alert Contact etc.

E-invoicing and Billing Category Specific Details

SIS allows the SIS Member to set-up Billing Category and e-invoicing specific parameters on the Member Profile which control the behavior of the SIS application at the time of processing.

Clearing House Specific Details

SIS allows view access to the Clearing House set-up details to the SIS Members. This information can only be updated by the respective clearing house operations team members.

Technical Details

The SIS application allows the SIS Members to store the login credentials of the ftp servers/iiNET where the output files needs to be provided.

2.3 User Set-up

The SIS platform allows different type of users to be configured in the system. These include:

1. SIS Member Users
2. SIS-Ops Users
3. ICH Ops Users
4. ACH Ops Users

△ Depending on the type of the user, the IS-WEB Menu structure and the Screens changes accordingly. The User profile details stored in SIS includes the name, location details, email id, contact number etc of the person. The email id of the user acts as the login id for IS-WEB.

In case of SIS Member Users, SIS-Ops creates a Member Super User account once the participation formalities are completed. This Member Super User can create other Users for the SIS Member.

2.4 Assign Permissions

The SIS Platform will assign the maximum permission allowed for a SIS Member User to the SIS Member Super User Account. The SIS Member Super User, at the time of creating other users, can assign permissions to the users. These include permissions for viewing/editing information on a particular screen, permission to perform some special operations on specific screens, permission to create other users etc.

The SIS application will have default templates to assign permissions, which can be used by SIS Member users to assign permissions. Member Users will also have the ability to create their own permission templates and apply them to their users.

The SIS application also provides a facility to copy the user permission profile from one user and replicate them on other users.

3. DATA TRANSMISSION

All files to and from SIS will be processed initially by iiNet on behalf of SIS. Files will be received by iiNet from all Members, and will be transmitted by iiNet to the SIS application. Once the file is received correctly by iiNet, iiNet will complete delivery to the SIS application. Any files to be transmitted to a Member will be sent by the SIS application to iiNet, and will be transmitted from iiNet to the Member.

Files from the Member must be pushed to iiNet, and files from iiNet to the Member may be pushed by iiNet or pulled by the Member at the Member's choice.

There are no fees for this service provided by iiNet for files transmitted from and to SIS, but usage will require separate acceptance of the iiNet Terms Of Use. Any added-value services provided by iiNet beyond transmission between the SIS Member and SIS are subject to iiNet's normal terms and conditions, and fees may be applicable.

4. RECEIVABLES PROCESSING

The SIS application will process the incoming invoices and supporting documents provided by the billing entities for all four Interline Billing Categories (Passenger, Cargo, Miscellaneous and UATP).

4.1 Invoice Data Processing

Input Possibilities

The SIS application allows the billing entities to provide invoice information in multiple electronic formats. In the case of Passenger and Cargo billings, the invoice information can be provided in a flat file based structure (IS-IDEC) or in an XML file format (IS-XML). Miscellaneous and UATP invoices can be submitted only in the IS-XML format.

Along with the electronic mode of invoice submission, SIS will also provide a facility to manually capture and review invoice information online over the internet, named IS-WEB. The table below details the support provided by SIS for different type of transactions within each Billing Category.

Table: Input possibilities for each Billing Category in SIS

Transaction Types	Input Option		
	IS-IDEC	IS-XML	IS-WEB
Passenger Billings			
Non Sample Prime Coupon Billings (including FIMs)	X	X	X
Non Sample Rejection Memos	X	X	X
Billing Memos and Credit Memos	X	X	X
Sampling Provisional Invoice (Form A/B)	X	X	–
Sampling Universe Adjustment (Form C)	X	X[2]	X
Sample Adjustments (Form D/E)	X	X	X
Sample Rejections (Form F and XF)	X	X	X
Correspondence	–	–	X
Cargo Billings			
Original AWB Billings	X	X	X
Rejection Memos	X	X	X
Billing Memos and Credit Memos	X	X	X
Correspondence	–	–	X
Miscellaneous Billings			
Original Invoice	–	X	X
Rejection Invoice	–	X	X
Correspondence Invoice	–	X	X
Correspondence	–	–	X
UATP Billings			
Original Invoice	–	X	X

On successful receipt of an incoming file, SIS generates a confirmation email and sends it to the billing entity. This email alert can be configured by billing entity using the Member Profile screen on IS-WEB.

In case of invoices captured over IS-WEB, SIS generates an email alert to the billing entity 24 hours before the billing period closure providing a list of open invoices yet to be submitted for further processing.

Data Validation

Invoice data provided by the billing entities will be validated by SIS. This process will ensure that the invoice data is of good quality and the billed entities can process the same without any issue within their internal systems. This process will take place upon receipt of each SIS billing file.

The different types of validation checks performed by the SIS application are as follows:

- ***File Construction checks:*** SIS will validate if the invoice files are created as per the defined file specifications, naming convention, duplicate files, compression logic, etc
- ***Field Format checks:*** SIS will check if data values have been provided for mandatory data elements, conditionally mandatory data elements if the condition is met, etc. It will also ensure that the data is provided as per the field format (e.g. numeric, alphabetic, date, etc) and as per the field length specifications (e.g. numeric field with a maximum of 5 digits)

[2] Form C data needs to be provided in Form C IS-XML file which is separate from the standard IS-XML file.

- ***Reference Master checks:*** Invoice data fields having standard reference data values are valid (e.g. From City field if populated should have a valid IATA city/airport code, etc)
- ***Interline Billing Rules checks:*** Some of the Interline billing rules defined in the RAM or ACH Manual of Procedure, such as possible duplicate billing check, outside time limit billings, minimum billing amount check for different type of transaction, etc.
- ***Settlement Information checks:*** SIS will validate the correctness of the Settlement details provided on the invoice if it needs to be cleared through a clearing house (e.g. Currency of Clearance information, Clearing House information, etc).
- ***Billing Audit Trail checks:*** SIS will check if the various stages of billing are linked together and there are no out of turn billings (e.g. validation of 'Previous Invoice number', 'Previous Billing Month', 'Previous Rejection number', 'Rejection Stage number' in case of Rejections etc)
- ***Computation checks:*** SIS will validate if billing amounts specified at various levels within the invoice add up together (e.g. the invoice total adds up to the sum of all Line Item totals, similarly Line Item total adds up to the sum of all Line Item details totals etc). The total of the line items must not vary from the invoice value by more than a small tolerance.
- ***Legal Requirement checks:*** SIS will validate if certain legal requirements are satisfied by the Billing Entity in the invoice data (e.g. invoice Number is unique for a Billing Member within a calendar year, VAT breakdown information is provided in the case that VAT amounts are billed in the invoice, etc)

Wherever possible, SIS will validate the entire file and identify all possible errors in the file. A validation report is generated at the end of this process and is provided to Billing Entity irrespective of the status of the validation. In case of errors, the Billing Entity can configure its Member Profile to receive an email alerting its contact about the details of the Validation error.

Invoice data captured using IS-WEB is validated at the time of data entry. SIS will alert the user in case invalid data in entered at the time of saving the information.

The SIS Platform does not validate the following:

- Whether the entity can legally bill the invoice through SIS
- Whether the billed amounts are correct
- Whether all required taxes are applied correctly
- Whether all required legal information of all countries in the world is provided

Error Handling

In case of validation error, SIS provides a facility to delete the erroneous invoices or the entire file through IS-WEB. For certain errors, SIS also provides an option of carrying out online correction on the IS-WEB. These correctable errors are errors related to reference data values such as invalid city/airport code, invalid tax code etc.

Invoices in an error status are not considered for further processing by SIS.

4.2 Supporting Document Management

Input Possibilities

SIS provides the facility for billing entities to supply supporting documents in electronic format in both batch and as online modes. At the time of invoice capture, billing entities can manually upload the supporting documents. SIS will store the uploaded supporting documents and link them to the invoice, or to the transaction within the invoice.

SIS supports 3 indexing options for submitting supporting documents in a batch mode. These are:

- Using folder name based indexing
- Using a CSV file based indexing
- Using an XML file based indexing

The formats are explained in the SIS Participation Guide.

Billing entities can use any of the options to submit the batch supporting documents to SIS.

On successful receipt of a batch supporting file, SIS generates a confirmation email and sends it to the billing entity.

Data Validation

SIS carries out certain sanity checks on the batch supporting document file before it is considered for processing. The different type of checks includes the following:

- ***File Construction checks:*** SIS will validate if the batch supporting documents files are created as per the defined file specifications, naming convention, duplicate files, compression logic, etc
- ***Index Information checks:*** SIS will validate the index information supplied with the batch supporting documents files and confirm if it is as per the defined specification.
- ***File Extension checks:*** SIS will validate the file extensions of the individual supporting documents and check if it matches with one of the supported neutral file formats. In case it is not a neutral file format, SIS will validate if any exceptions for supporting document file types have been defined in the Member Profile of the billed entity for acceptance. If it is not an exception, SIS will delete the supporting document file from the system.

Wherever possible, SIS will validate the entire file and identify all possible issues in the batch supporting document file. A validation report is generated at the end of this process and is provided to the billing entity.

Automated Linking of Supporting Documents

The SIS application will carry out auto-linking of supporting documents provided in a batch mode to the corresponding billing record. This linking will be based on the Index information supplied in the batch supporting document file. Invoices which are successfully validated will be considered for automated linking. SIS will take care of any timing issues in case of automated linking if the supporting document file is provided prior to the invoice being successfully validated.

For cases where the SIS application is not able to automatically link the supporting documents, SIS provides a facility by which the billing entity can update the linking information on IS-WEB and manually trigger the linking process.

4.3 Value Determination, Auto-Billing and Billing Value Confirmation

Value Determination

This is an optional service provided by SIS in conjunction with A&A which can be utilized by Passenger billing entities that store prorated coupon values within ARC COMPASS®.

As part of this service, SIS accepts Usage Files (modified Record 50 file format as defined in the SIS Participation guide) from billing entities requesting prorate values for coupons utilized by them. SIS validates the file format and forwards the Usage File to ATPCO for further processing. The processed information is provided by ATPCO back to SIS. SIS forwards the output files provided by ATPCO to the billing entities.

Internally SIS keeps track of which transactions were provided by the billing entities for processing and which transactions were processed and returned by ATPCO. On a daily basis SIS creates a report highlighting transactions where a response is not provided by ATPCO as per the defined timelines, and provides it to the billing entities.

Auto-Billing

Auto-Billing is an optional service provided by SIS in conjunction with A&A and is an extension of the Value Determination process.

As part of this service, SIS will store the prorate records received through the Value Determination process and generate invoices on behalf of the Billing Entity. On a daily basis SIS will generate a Revenue Recognition File (File Format defined in the SIS Participation Guide) containing the billing records of coupons included in the Auto-Billing Invoices. This Revenue Recognition File along with

the optional ISR data is forwarded to the billing entity by SIS. SIS allows the billing entity to correct/update the values of the Auto-Billing invoices though the IS-WEB. Any update made on IS-WEB is reported back to the billing entity in the next Revenue Recognition File.

The Auto-Billed invoices are automatically closed and finalized by SIS and processed further like any other IS-IDEC/IS-XML invoices. At the end of the billing period, SIS generates an IS-IDEC file for the billing entity called Invoice Posting File which includes details of all Auto-Billed invoices. The billing entity can use it to carry out any account postings for such invoices within its Revenue Accounting/General Ledger System.

Billing Value Confirmation

This is also an optional service provided by SIS in conjunction with A&A. This service validates the Passenger billing values against the prorate values stored within ATPCO.

SIS generates a Billing Value Confirmation file for passenger prime billing coupons where both the billing entity and billed entity are subscribers to this service. This file is forwarded to ATPCO for further processing. ATPCO validates the billing values with the prorate values stored within its database. Any exchange rate conversions of the prorate values as per the billing month will be done by ATPCO before comparing the values. The results of the comparison are updated by ATPCO and provided to SIS. SIS updates the comparison results within its Billing Record Database.

SIS automatically generates a Billing Value Confirmation report at the end of each billing period and provides it to the billing and billed entities.

4.4 Digital Signature Services

This is an optional service provided by the SIS application.

Digital Signature Application

SIS offers digital signature (DS) application service through a trusted digital signature service provider (currently TrustWeaver). Based on the instructions provided by the billing entity, SIS creates from the SIS-format invoice data an invoice subset file in PDF or XML format with the necessary legal and invoice information fields. This invoice subset file is forwarded to a trusted DS service provider in order to apply the appropriate digital signature. The file is sent immediately unless the file is incomplete (awaiting attachment). If there are attachments awaited, the file is not sent until all attachments have been uploaded and matched, or the billing deadline is reached, at which point the number of attachments reported is updated to reflect the number that are actually available at that time. The invoice is then sent for digital signature. After applying the digital signature, SIS receives the invoice subset file and stores it in its Central Repository. This digitally signed file is made available by SIS as one of the outputs to the billing entity at the end of the billing period, based on the configuration of the Member Profile. The file can also be downloaded online over the IS-WEB.

4.5 Settlement Services

The SIS application provides interfaces with industry clearing houses thus enabling automatic settlement of billed invoices as well as other clearing house related services.

Settlement Information

The SIS application interfaces with two clearing houses: The IATA Clearing House (ICH), and the Airlines Clearing House (ACH). Based on the instructions provided by the billing entity, SIS generates a summary statement of the billed invoices and forwards it to the respective clearing house for settlement. In case of ICH, SIS generates claim files every 10 minutes whereas in case of ACH the settlement information is generated and passed only once at the billing period closure.

Suspended Member Billing Management

SIS supports billings from or against entities that continue in business but have been suspended from the clearing house. The billing entities can continue to send invoices to be routed through the clearing house or for bilateral settlement. In case of billing from/to suspended members involving ICH, SIS will flag the invoices as “Suspended” in the summary settlement statement and forward them to ICH. The ICH will record this information in accordance with its procedures. In the case of

billing from/to suspended members involving ACH, SIS will not include such invoice details at the time of creating the summary settlement statement, and no record will be retained by the ACH. When creating the SIS-Format output (IS-IDEC, IS-XML or IS-WEB), SIS flags such invoices as "Suspended" and forwards them to the billed entity along with the other invoices.

In case of re-instatement of the suspended member, SIS provides the functionality for the billing entities to re-submit their claims and settle through the clearing house any outstanding amounts that arose after suspension. SIS also provides a report which helps the billing entities to manage the invoice claims made during the suspension period.

Handling Late Submission Billings

SIS supports processing of invoices of closed billing periods for a short duration of time, immediately after the closure of the billing period. The designated person identified in the Member Profile can request invoices to be considered for Late Submission. On acceptance of such request by the clearing house, the invoices will automatically be considered for settlement. Clearing houses may charge a fee for such submissions.

4.6 Reports, Alerts and Outputs

Processing Dashboard

SIS has an online dashboard on IS-WEB which provides visibility of the status of processing of receivable invoices. There are 2 views provided by the dashboard:

- *File Level View:* This view provides the status of processing of files submitted to SIS.
- *Invoice Level View:* This view provides the status of the receivable invoices processed in SIS. The status of the intermediate stages of invoice processing can also be viewed and downloaded by the SIS Member.

Reports

SIS provides reports to its members based on the receivables data which can be used to analyze billing trends and volumes. These reports can be queried using a number of different criteria and saved in PDF or Microsoft Excel format.

Alerts

SIS generates a number of alert messages to the SIS Member. These alert messages are sent by email to the contacts setup in the Member Profile. Some of these alerts are listed below:

- *Profile data update alert:* An alert email message is generated every time a change is made to the Member profile details. It is also generated when a post-dated change made on the Member profile becomes effective.
- *Other Members Invoice Reference Data Update alert:* An alert message is sent with an attached CSV file providing details of changes made by other SIS Members on their location information. This update can be used by the SIS Members to synchronize the new location details within their receivables system.
- *DS failure alert:* An alert email message is generated in case SIS Platform was unable to apply Digital Signature on a particular invoice.
- *File Receipt alert:* An alert email message is generated by SIS whenever a file is received by the platform for processing. This alert can be set up on the Member Profile for incoming files related to individual billing categories.
- *Validation Error alert:* An alert email message is generated whenever an invoice file fails in the validation process. This alert can be set up on the Member Profile for an individual Billing Category. The Validation report is attached along with the alert email.
- *Open invoices alert:* An alert email message is generated 24 hours before the billing period closure informing the user about open invoices on IS-WEB, yet to be submitted for processing. A list of Open invoices is also attached with this email.

Output Information

SIS application generates the following outputs from the receivables data provided by the Member:

- E-invoicing related files, which include
  - Invoices in PDF format
  - Detail Listings in csv or pdf format
  - Digital Signature files
- Memos (in case of Passenger and Cargo billings)
  - Rejection/Billing/Credit Memo details in html format

Based on the preference defined in the member profile, SIS automatically creates a zip file and includes in it the above mentioned files for all invoices fully processed in that period. The above mentioned outputs can also be downloaded manually from the IS-WEB for individual invoices.

In case of invoices submitted by 3rd parties on behalf of SIS Members (e.g. invoices raised by IATA for Call Day Adjustments; invoices submitted by ATCAN for UATP claims), SIS provides the billing entity with the option to generate an IS-XML output file at the end of each billing period. This file can be used to carry out account adjustments within the Receivable system of the billing entity.

SIS provides an option via the member profile to automatically generate a summary report with the listing of all invoices fully processed in a particular billing period. This report can be used by the billing entity to synchronize the processing status of invoices within its Receivable system.

5. PAYABLES PROCESSING

The processed invoices of the Passenger, Cargo, Miscellaneous and UATP Billing Categories are made available by the SIS Platform to the SIS Member at Output File Generation Time as shown in the SIS Calendar.

5.1 Invoice and Supporting Data Management

Based on the setup in the Member Profile, the SIS Member can receive the following from SIS for Payables processing:

- SIS-Format Invoice Files: SIS groups the payable invoice information as per the Billed Entity and Billing Category level and generates invoice files as per the format requested by the billed entity. The SIS Member has the option of selecting both IS-IDEC and IS-XML format (if applicable for the Billing Category) in the Member Profile and SIS will generate two separate zip files one with invoice information in IS-IDEC format and another in IS-XML format.

  The Payable invoices can also be reviewed over IS-WEB.

  In case of Passenger Sample billings, SIS supports an option to generate a consolidated SIS-Format Payables file containing Sample Provisional Invoices raised by other SIS Members on a monthly basis. This file will be in addition to the weekly SIS-Format billing file generated for the billed entity and will be zipped separately.
- Offline Archive Files: At Output File Generation Time as defined in the SIS Calendar, SIS generates the following additional output files and groups them as per the Billed Entity and Billing Category into separate offline archive files:
  - E-invoicing related files
    - Invoice in PDF format
    - Detail Listings in csv or pdf format
    - Digital Signature files
    - Digital Signature Verification log files

- Memos (in case of Passenger and Cargo billings)
  - Rejection/Billing/Credit Memo details in html format
- Supporting Documents

An XML index file is also provided having references for each file provided in the Offline Archive. This XML file is used by the SIS Member to automatically read and link the contents of the Offline Archive within its internal payables system.

The above outputs can also be downloaded for individual invoices manually over the IS-WEB. They are kept for 60 days, and then deleted.

An alert email can be configured on the Member Profile at a Billing Category level to be triggered whenever the output files are generated and available to download. In case of a SIS-Member opting for IS-WEB, this alert will denote that the invoices are available for review on IS-WEB.

5.2 Rejections of Incoming Billings

SIS enables rejection of incoming billings either via file upload using the IS-IDEC or IS-XML formats, or by manual entry into the IS-WEB. Rejection processing can only take place once the Billing Output file has been received from SIS at the end of the clearance period. It is not possible to reject an incoming invoice in the same period as it was issued.

The SIS application will check that rejections are in sequence, and contain the required information, and will not permit rejections beyond the limits defined in the RAM or the ACH Manual of Procedure.

Rejections are only possible while the billing or rejection to which it refers remains live in SIS. Billing data in SIS is deleted at the expiry of the relevant billing time limit defined in the RAM or ACH Manual of Procedure, plus a system-defined period, normally set at two months after the deadline (e.g. 2nd rejection is no longer possible after 6+2 months from issue of the 1st rejection).

5.3 Process Invoices on IS-WEB

The SIS Platform allows SIS Members to review the Payable invoice and transaction details on the IS-WEB. It also allows the user to view supporting documents linked to the invoice/transactions within the invoice. SIS maintains an audit trail of all invoices/transactions within the platform so that the complete billing history of any invoice/transaction can be viewed at any time.

SIS allows Rejection Invoices/Memos to be raised weekly against Payable invoice transactions via the IS-WEB once received in the SIS outward file. The transaction details selected by the SIS Member when raising the Rejection Invoices/Memos are automatically carried forward thus reducing the data entry effort to some extent.

5.4 Digital Signature Services

This is an optional service provided by SIS.

Digital Signature Application

SIS allows billed entities to configure the application of Digital Signature on Payable Invoices on the Member Profile. Based on the location details specified on the payable invoice, if it matches the profile set-up of the billed entity, SIS triggers the process to apply digital signature as explained in section 4.4.

Digital Signature Verification

SIS provides an option whereby the billed entity can request verification of the digital signature applied on Payable Invoices, via the Member Profile. A verification log file is created by this process which contains the status of the applied digital signature.

5.5 Reports

SIS provides a number of reports to its members based on the payables data which can be used to analyze billing trends and volumes. These reports can be queried using a number of different criteria and saved in PDF or MS Excel format.

6. CORRESPONDENCE MANAGEMENT

As per the Interline billing rules defined in the RAM and ACH Manual of Procedure, once the maximum number of allowed rejections for a billing has been reached, the entity which received the last rejection can only continue the dispute by initiating correspondence. SIS will not permit further rejections after the limit has been reached.

6.1 Generate Correspondence

Once the maximum number of allowed rejections has been reached, the SIS application provides a facility by which the SIS Member, who received the last rejection, selects the rejection transaction/invoice on IS-WEB and initiates correspondence. The SIS application automatically populates the data in the correspondence screen based on the Member Profile information. SIS automatically generates a correspondence reference number which remains the same until the end of the correspondence cycle. SIS provides an option to the SIS Member to attach supporting documents to the correspondence.

SIS provides a facility by which the SIS Member user can save the correspondence in the draft stage and work on it later. SIS also provides a facility by which, if a user does not have the permission to send correspondence, can mark the correspondence as “Ready to Submit” and the supervisor can review, edit (if required) and send the correspondence.

6.2 Receive Correspondence

When a correspondence is sent via SIS, an email notification is generated and is sent to the Correspondence Alert contact defined in the Member Profile for the specific Billing Category. The email only contains a URL reference, which on clicking, will open up the IS-WEB Correspondence screen (note: it may be necessary for the user to modify their junk/spam filters to enable these communications to be viewed/actioned). On reading the correspondence if the SIS Member wants to continue with the correspondence process, SIS provides a facility by which a reply correspondence is generated and the SIS Member user is allowed to enter the details and send it to the interline partner.

SIS ensures that there is no out of turn correspondence done by the SIS Member User.

6.3 Grant Authority to Bill for Correspondence

SIS provides a facility where the SIS Member who received the 1st correspondence can grant an Authority to Bill when responding to the received correspondence. If the interline partner who received the Authority to Bill Correspondence is not satisfied with the amount for which the authority is granted, it can continue with the correspondence process and the Authority will be considered null and void.

If the interline partner receiving the authority to bill accepts the amount for which authority is granted, the Member is expected to raise a Billing Memo/Correspondence Invoice and claim the amount for which the authority is granted. SIS validates the amount of such Billing Memos/ Correspondence Invoices and matches it with the Authority amount. In case the two are not matching and the difference is more than the allowed tolerance, the invoice will fail in the Validation process.

6.4 Expiry of Correspondence Cases

SIS tracks the expiry dates of open correspondence cases in the system as per the rules defined in RAM/ACH Manual of Procedure. In case the party that initiated the 1st correspondence does not respond to a received correspondence by the expiry of the time limit, the Correspondence case is closed by SIS automatically with no further recourse through SIS for that particular case.

Similarly if an Authority to Bill was granted and the SIS Member fails to raise the Billing Memo/Correspondence Invoice by the expiry time limit, SIS will close the correspondence case with no further recourse.

In case the party who received the 1st correspondence fails to respond to a received correspondence by the expiry time limit, SIS will mark the correspondence case as Expired. The SIS Member who caused the expiry will not be allowed to respond to the correspondence any further by SIS. The other party has the right to raise a billing memo/Correspondence Invoice equal to the amount stated in the last correspondence sent which had expired. SIS validates the amount of such Billing Memos/Correspondence Invoices and matches it with the amount of the last correspondence. In case the two are not matching and the difference is more than the allowed tolerance, the invoice will fail in the validation process.

In the above case if the SIS Member fails to raise the Billing Memo/Correspondence Invoice by the expiry time limit, SIS will close the correspondence case with no further recourse.

6.5 Alerts and Reports

Alerts

SIS generates a number of alerts for the following correspondence cases;

- An email alert is generated and sent to all Correspondence Alert contacts when a new correspondence is received
- △ 72 hours before expiry of a received correspondence, an alert is generated by SIS informing the Correspondence Alert contacts
- △ 72 hours before expiry of a draft correspondence, an alert is generated by SIS informing the Correspondence Alert contacts
- For any received correspondence which has the Authority to Bill flag and a Billing Memo/Correspondence Invoice has not yet been raised two days prior to the expiry of this Correspondence

Correspondence Alert Contact can be different for each Billing Category.

Reports

SIS provides a Correspondence Status report allowing the users to track the details of the correspondence within the system. This report can be downloaded in PDF or Excel format.

6.6 Download

SIS provides an option to download the correspondence case with the complete mail trail in PDF format.

7. SYSTEM REPORTS

SIS provides a number of reports to support the member. These include:

- SIS Usage Report
- Member Details Report
- Contact Details Report
- Suspended Billings Report

- PAX Receivables–Supporting Documents Mismatch Report
- PAX Correspondence Status
- PAX Receivables–RM BM CM Summary
- PAX Payables–RM BM CM Summary
- PAX Receivables–Billing Value Confirmation Analysis
- PAX Payables–Billing Value Confirmation Analysis
- Cargo Supporting Attachments Mismatch Report
- Cargo Submission Overview–Receivables
- Cargo Submission Overview–Payables
- Cargo Interline Billing Summary–Receivables
- Cargo Interline Billing Summary–Payables
- Cargo Rejection Analysis–Receivables
- Cargo Rejection Analysis–Payables
- Correspondence Status Report
- MISC Correspondence Status
- MISC Payables Invoice Summary Report
- MISC Receivable Invoice Summary Report
- UATP-ATCAN Statement

A full list is available in the SIS Participation Guide and SIS User Guide.

8. GLOSSARY

Term	Definition
ACH	ACH stands for Airlines Clearing House. It is the ATA's Clearing House for Interline Billings.
ACH Recap Sheet Submission Deadline	This is the time by which ACH members should submit their Claim details (Recap Sheet) to the Clearing Bank.
A&A	A&A stands for ATPCO and ARC. A&A is the organization formed by ATPCO and ARC to support the First & Final™ process.
ARC	Airlines Reporting Corp. ARC operates COMPASS® which houses transaction and prorate data for the purposes of settlement.
ATA	(Air Transport Association)–The trade group for U.S.-based airlines.
ATPCO	Airline Tariff Publishing Company. ATPCO, amongst other services, operates the Sales Exchange process whereby sales for First & Final™ transactions are extracted, prorated, and sent to the uplifting carrier.
Audit trail	A chronological sequence of audit records.

Term	Definition
Auto Billing	A proposed feature of SIS whereby a billing carrier is able to submit a list of uplifts. SIS will then find the prorate (either a stored own prorate or an NFP) and create the necessary billing, settlement, and invoice files. A pro-forma invoice is sent to the billing carrier daily, and invoices are sent to the billing and billed carrier on settlement.
Batch Key	Batch Key is a set of data elements that uniquely identifies an Invoice or a transaction that needs to be linked with supporting documents.
Billed Entity	The Billed Airline or Supplier
Billing Category	The Category of the Interline Billing Invoice. There are 4 Billing Categories: Passenger, Cargo, Miscellaneous and UATP
Billing Date	The Billing Date field refers to the month period of settlement. This field is referred extensively in RAM chapter A13 in case of Miscellaneous billings.
Billing Entity	The Billing Airline or Supplier
Billing Entity Code	The Numeric code of the Billing airline or the Alpha numeric code of the Supplier
Billing Period	Billing Period refers to the Period of the Clearance Month used for billing. As the current interline settlement is on a weekly basis, there are 4 periods in a month. The billing period is represented as 01, 02, 03 and 04.
Billing Record Database	This is the data store within SIS which will maintain the Invoice data provided by SIS Participants in SIS-Format. The data is kept in the system till the time the transactions are expired.
BM	Billing Memo. Applicable in case of Passenger and Cargo Billings
Breakdown Record	A Breakdown record provides additional information regarding the certain data elements present in the parent record.
BSP	Billing and Settlement Plan–An IATA service for the settlement of ticket revenues between agents and carriers. BSP fees can appear on interline billing invoices
CASS	Cargo Account Settlement Systems–An IATA Service designed to simplify the billing and settlement of accounts between airlines and freight forwarders
Central File Repository	Central File Repository is the data store within SIS which maintains the input and output files including the Supporting documents for the billing transactions.
Charge Category	The major types of Miscellaneous Invoice billed between carriers
Charge Code	The sub group within the Charge Category which identifies the different reasons for the Miscellaneous Invoice claim.
Clearance Month	It represents the month of Interline Billing.
CM	Credit Memo
CSV File	Comma separated file
Currency of Billing	In case of Passenger, Cargo and UATP Billings, the Currency of Billing is the currency in which the total Invoice values are converted. This Currency of Billing can be GBP, USD or EUR in case of ICH Invoices and USD or CAD in case of ACH Invoices.
Currency of Listing	The Currency in which the billing transactions are listed in case of Passenger, Cargo and UATP billings. The Currency of Listing can be any local currency.

Term	Definition
Detailed Validation	This is the second phase of the SIS-Validation process in which the billing data is loaded in the Billing Record Database and each and every data element in the billing data is validated.
Digital Signature	Digital Signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit
DS	Digital Signature
E-Archiving	E-archiving is an optional service provided by SIS. This service allows Participants to store digitally signed invoices in an external Legal archive for a longer period as required by the local regulations.
EST	***Eastern Standard Time***
F&F	**First & Final**–Process in which two carriers agree to use a Neutral Fare Proration engine for interline billings. In agreeing to settle on a First & Final basis, they are also agreeing that rejects based on prorate values are not permitted.
File Naming Convention	Rules followed for construction of the file name
GDS	***Global Distribution System***
GL	General Ledger
Hard Cut Over	The Phase in the SIS Migration when the old IDEC processing will be switched to the SIS Platform from ATPCo.
HTML files	Files in Hypertext markup language. HTML is a structured file format used in websites, which includes tags.
ICH Period Closure Day	This is the time by which ICH Members should submit their invoices to SIS to be sent to ICH and considered for settlement.
Index File	An index file contains the mapping information of the various supporting documents and its corresponding Batch Key. There are two formats of index files supported by SIS. These are CSV and XML
IS or SIS	Integrated Settlement Integrated Settlement is the name for the collection of systems which provide the functionality behind Simplified Invoicing and Settlement (SIS). The term SIS is also used interchangeably.
SIS Calendar	The Calendar used by SIS to trigger various automated processes. It also has deadlines for some of the processes impacting the end-users of SIS.
SIS Calendar Billing Output Generation Date	This is the date and time stamp by which SIS will generate the billing output files and keep it ready for download,
SIS Format	SIS Format is a generic term used to define Invoice data provided to SIS in either automated formats like IS-IDEC or IS-XML or manually over IS-WEB
IS-IDEC	IS-IDEC is the new flat file specification defined for Passenger and Cargo invoice data billing and settlement through SIS.
IS-WEB	IS-WEB is the online user interface of the SIS System. It allows users to capture data, pull out reports, as well as configure the Member profile information.
IS-XML	IS-XML is the new interface file format defined for PAX, CGO MISC and UATP. This file format is based on the existing IATA Aviation Invoice Standard.

Term	Definition
ISC	Interline Service Charges
ISR	Industry Standard Record (enhanced version of TCN–Transmission Control Number data). A&A value determination process returns prorate values files to SIS, and these files are referred to as ISR in the context of this document. The prorate values file may or may not contain sales data. In A&A/ATPCO terminology, ISR is a term used only for sales data.
JPEG Image files	***Image files in JPEG*** (Joint Photographic Experts Group) format.
Late Submission	Invoices submitted after the SIS Submission Deadline but within the Late Submission Acceptance Window to be considered for settlement in the previously close period
Late Submission Acceptance Window	Time window in which Late Submission can be submitted.
Location Code	Code of the Member's location.
Location IDs	User defined code that uniquely identifies the Member's location in the Member Profile.
Member Profile	Centralized functionality that enables the participants to: 1. Create and Manage Users of SIS 2. Configure the various processes within SIS 3. Set default values to be used at the time of processing 4. Set up Third Party preferences, such as parameters applicable to ACH, ICH, A&A
NFP	Neutral Fare Prorate–A prorate created by a “neutral” party, as currently used within First & Final™ settlement. Because of their neutral nature, NFPs are less likely to get rejected by the billed carrier, even outside of First & Final™. In the future, NFP values will be available to all carriers that wish to use them.
Partially Migrated	Migration to SIS can be carried out in Phases. In case of Passenger billings the Billing entities have the option of migrating Prime billing first, then rejection and then Sampling. Any Billing entity who has not completed all phases of migration is referred to as Partly Migrated
Participant	An Airline or a Non Airline Entity who is a signatory or a potential signatory to SIS Services.
Payables	Billing received from other interline partners for a billing period is referred to as Payables
PDF	***Portable Document Format***
Prime Billing	First time billing or billings of original documents (like coupons, air waybills) are referred to as Prime Billings
Processing Dashboard	Module in SIS for: • Viewing processing details • Submitting of invoices/files for late processing • Increment the period of the invoices
Protest	Protest is the action taken by a billed entity against an erroneous billing done by a billing entity before the amount in error is settled by the Clearing House.
RAM	Revenue Accounting Manual

Term	Definition
Reason Code	A two character code to be assigned to each Rejection Memo, Billing Memos as well as Credit Memos to indicate the reason for raising a Memo;
Receivables	Invoices billed to other interline partners is referred to as Receivables
Record 50 file	Record 50 is the file used today in First & Final™ for Post Sales Processing. This file has been modified in SIS is now called “Usage File”.
Reference Data	Reference data relates to the basic legal information of the Billing and Billed entity. This includes details like the Company Legal Name, Tax Registration ID, Address details etc.
RM	Rejection Memos
Sanity Check	This is the first phase of SIS-Validation, where a file is checked for Construction errors. If an error is encountered in this phase the entire file is rejected by SIS.
Settlement Method Indicator	The field Settlement Method Indicator in the Invoice data drives the Settlement process of the Invoice.
SIS	Simplified Invoicing and Settlement (SIS)
SIS Operations	User for SIS operations
SITA	Provider of global information and telecommunication solutions for the air transport industry.
SPA	Special Prorate Agreement
Submissions Open Date	The date and time from which SIS starts accepting Billing Files for a particular Clearance period
Supporting Attachments	The additional documentation provided to support interline billing claim. The Supporting Attachments needs to be provided in electronic format
Supporting Attachments Linking Deadline	The date and time stamp by which the system will stop manual and automated linking of supporting documents for the clearance period
TIFF Image files	Tagged ***Image File*** Format (TIFF) is a ***file*** format for storing images.
Time Stamp	Sequence of characters, denoting the date and/or time at which a certain event occurred
UATP	Universal Air Travel Plan, an Industry owned charge card
Usage File	The modified Record 50 file is now called Usage File. This is used as an input to SIS to carry out the process of Value Determination and/or Auto-billing
VAT	Value added tax

ATTACHMENT E—SERVICE LEVEL AGREEMENT

SIS—Service Level Agreement

1. System availability

△ (a) The Service will be available on a 24 hour, 7 days per week basis, with system up-time averaging 99.50% on a rolling annual average, excluding weekends.[1] Maximum unplanned outage should not exceed 4 hours.

2. Processing

△ (a) IS-IDEC and IS-XML files received will be processed to Clearing House submission if applicable within twenty four hours of receipt and within four hours in 99.85% of cases.

⊗

△ (b) Online entry other than for report generation or file transfer should receive a response within 3 seconds target in 97.50% of transactions based on an end to end bandwidth of at least 256kb.

3. Helpdesk availability

(a) IATA and its service provider will provide access to a 24-hour web based helpdesk, 7 days per week.

4. Fault reporting and clearance

(a) Communication may be via web interface (primary solution) or via email (back-up).

(b) If a fault is identified

(i) by the Participant:

(i) The Participant will notify IATA through its Help Desk facility and indicate the severity of the fault in accordance with the categorizations below.

(ii) If the fault is confirmed, the IATA Help Desk will validate the severity classification, and communicate immediately in case of a Severity 1 issue. In case the incident is escalated, a second e-mail notification will be sent out reporting its escalation and prioritization.

(iii) All incidents will be recorded and the Participant will receive an e-mail notification reporting a unique tracking number associated with each case within minutes after the incident was logged via the web based solution.

(iv) If the fault is deemed by IATA Help Desk to affect other Participants, IATA Help Desk will notify the Participants of the fault and recommend any temporary corrective action.

(ii) by IATA or its service provider:

(i) The IATA Help Desk will determine the severity of the fault and in case of a Severity 1 issue, communicate immediately to the Participant or all Participants.

(ii) Communication could be via the IS-Web portal.

(c) IATA Help Desk will:

(i) Generate a fault report to the Participant or all Participants, as appropriate, after full assessment of the fault (for Severity 1 issues).

[1] For the purpose of calculation, only Saturdays are considered as weekend.

(ii) In the course of defining the proper resolution, the Participant may be requested to provide any additional information to the IATA Help Desk in a timely manner to enable correction of the fault/problem.

(iii) Communicate a suitable fix for either data or processes or provide a workaround for other than trivial cases (severity 4). The time allowed will be dependent upon the severity of the case.

(iv) Notify the Participant or all Participants, as appropriate, once the fault has been fixed.

(d) Fault categorization and resolution timelines

1. IATA Help Desk will validate or determine the severity of the case based on the following definitions:

Showstoppers (Severity 1): Showstopper faults are those which prevent global use of the application software or which stop an operational function of application globally, thereby preventing the users from completing essential operations. IATA will endeavour to provide a resolution, either in the form of a workaround or a patch in that order of priority, within six (6) hours. However, if more time is needed, this will be advised to the respective users. Until April 2013, the legacy processes will be maintained and can be used as fall back option. Once an alternative is provided or normal functioning of the application is instituted, the IATA Help Desk will inform the participants and the Showstopper will be considered resolved.

The following will qualify as Showstopper faults:

- Complete SIS platform is down
- Submission of billing data is not possible
- Settlement files cannot be created or are incorrect or do not arrive at their destination within the SIS perimeter
- Output billing files cannot be created or are incorrect or do not arrive at their destination within SIS perimeter
- Invoices cannot be digitally signed
- Invoices do not contain intended values, or referential integrity is compromised
- Billing data captured through IS-Web do not contain intended values, or referential integrity is compromised
- Processing times for files are greater than 2 hours max to load and validate files for non-peak loads and 4 hours max for peak loads.
- Response times for manual input are greater than 8 seconds for delivery of high complexity operation pages.
- Users unable to log on to SIS due to problems accessing the platform (excluding invalid/lost/expired log-ons)
- Migration functionality inoperative (IDEC functionality, IS-IDEC conversion, etc)
- Security breach deemed to put SIS at risk.

Major (Severity 2): Major defects are defined as those which impact a specific module within the system and for which workarounds are available, or prevent a non-core system process to be successfully completed. IATA will endeavour to provide a resolution, in the form of a workaround, within 1 Work Days (*).

In the context of SIS, the following will qualify as Major defects:

- Web Analysis reports cannot be viewed/downloaded
- Alerts are not/incorrectly delivered
- Service usage report incorrectly produced by the SIS application.

Minor (Severity 3): These are faults where one or more functions in the application software are not working as normal or the SIS application's behavior deviates from expected functionality, but these do not affect the operation.

Trivial Defects (Severity 4): Trivial Defects are defined as those which do not affect the functionality of the SIS application and are cosmetic in nature. These will be addressed in future releases as per section 6 in the SIS Participation Agreement.

2. IATA will endeavor to resolve faults reported as per the following table from the time it is allocated.

Fault Severity	**Required Resolution Time (could be via workaround)**
Showstopper (severity 1)	6 Hours
Major (severity 2)*	1 Work Days
Minor (severity 3)*	10 Work Days
Trivial (severity 4)	Next planned Release

* These fault severity items will be responded to during 'Work Days'. "Work Day" is defined as 09:00 hrs to 18:00 hrs EST/EDT, Monday to Friday, excluding IATA Montreal company holidays.

(e) The Participant will be able to access the status of the report on their incident(s) at any time via the internet in accordance with Attachment D.

5. Disaster recovery plan, Back-up and recovery processes

(a) During the Term of this Agreement, IATA shall maintain a written Disaster Recovery (DR) Plan ("**Plan**") and the wherewithal to implement such Plan.

(b) IATA will test the Plan annually and produce a report containing the results of the test and recommendations for improvements, if any, to the Plan.

(c) IATA will maintain a back-up process sufficient to ensure that the service is restored within 6 hours of DR site invocation in case of disaster, with not more than 3 hours of submission data needing retransmission by the Participants.

(d) The Plan will provide a 3 hours switchover from the Primary site to the DR site.

(e) The restoration for full service operations will be completed within 6 hours after a catastrophic failure.

(f) The response time of this SLA will not apply when the Service is run from the DR site except for resolution of Severity 1 faults.

ATTACHMENT F—PARTICIPANTS IN THE AGREEMENT

1. TABULATION OF PARTICIPANTS

Please refer to www.iata.org/SIS for a current version of the Participants list.

ATTACHMENT G—EU STANDARD CONTRACTUAL CLAUSES

EU Standard Contractual Clauses for processing between an EU controller and non-EU processor (and sub-processor):

ONLY APPLICABLE TO SIS PARTICIPANTS WHO ARE SUBJECT TO EUROPEAN DATA PROTECTION LAWS.

PARTICIPANT TO CHOOSE BETWEEN **OPTION A** OR **OPTION B**

OPTION A:

EU Standard Contractual Clauses for processing between IATA and Participant (including the EU Standard Contractual Clauses for processing between IATA and Sub-processor. A signed copy is available upon request).

OPTION B: (for use only in jurisdictions where a tripartite agreement is required):

EU Standard Contractual Clauses for processing between IATA, Participant and Sub-processor.

OPTION A: EU Standard Contractual Clauses for processing between IATA and Participant:

Standard Contractual Clauses (processors)

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

Name of the data exporting organization:

.....

Address:.....

.....

Tel.:.....; fax:.....; e-mail:.....

Other information needed to identify the organisation

.....

(the data **exporter**)

And

Name of the data importing organization:

INTERNATIONAL AIR TRANSPORT ASSOCIATION
Address: 800 Place Victoria. P.O. Box 113, Montreal, Quebec, Canada, H4Z 1M1

Tel: 1 514 874 0202

(the data **importer**)

each a “party”; together “the parties”,

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

HAVE FURTHER AGREED that the data importer may utilise a sub-processor, as envisaged by these Clauses, and may enter into separate clauses with such sub-processor, a copy of which shall be provided to the data exporter to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the personal data specified in Appendix 1.

Clause 1 Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) *'the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the sub-processor'* means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 Details of the transfer

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

Clause 3 Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Clause 6 Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

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

   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7 Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9 Governing Law

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

Clause 10 Variation of the contract

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

Clause 11 Sub-processing

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

Clause 12 Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

[3] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

On behalf of the data exporter:

Name (written out in full): _____

Position: _____

Address: _____

_____

_____

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

(Signature)

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Adina Minculescu, International Air Transport Association

Position: Head, e-Invoicing Services, GDC

Address: 800 Place Victoria, P.O. Box 113

Montréal, Québec H4Z 1M1

Canada

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

(Signature)

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

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

Sending personal data to the data importer to support and if required validate the invoices submitted for payment (using the interline billing and settlement solution provided by the data importer to the data exporter and third parties).

Data importer

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

Receiving personal data from the data exporter to support and if required validate the invoices submitted for payment (using the interline billing and settlement solution provided by the data importer to the data exporter and third parties).

Data subjects

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

Airline passengers; Crew/Staff members of the data exporter or its counterparts.

Categories of data

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

Some or all of the following: passenger name, gender, date of birth, age, frequent flyer number, contact details, payment card data (masked in accordance with Payment Card Industry Digital Security Standard (PCI-DSS) specifications) and the special categories of data listed below.

Special categories of data (if appropriate)

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

Sensitive/special personal data that is associated with a charge to the customer such as medical information (if for example a charge for oxygen applied and the personal data explicitly or implicitly referenced a medical conditions).

Processing operations

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

Personal Data to be used where required to support and validate the accuracy of charges to be billed and settled between the data exporter and third parties.

Order Control

The Data Exporter has the right to carry out an inspection at the Data Importer's office at any time. In the course of the inspection the Data Importer shall give the Data Exporter reasonable assistance including but not limited to access to any necessary information and documentation and access to premises. In particular, the Data Exporter has the right to inspect the Data Importer's compliance with all technical and organizational measures.

DATA EXPORTER	DATA IMPORTER
Name:	Name:
Authorised Signature:	Authorised Signature:

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

1. Access control

Below are the access control mechanisms:

(a) Access card readers are in place at all areas of building.

(b) Access to secure areas (for e.g. access to data centre) are protected by dual authentication comprise of Biometric and access card reader.

(c) Door Security is covered through access card reader along with 4 digit PIN Code.

(d) Environmental and Physical security includes CCTV surveillance cameras, Alarm Systems, Sprinklers, Smoke Detectors.

2. Accession control

Following procedures are implemented

(a) Strong Password policy is set for user authentication.

- Base System Software Password Policy:

  Minimum 8 characters password with combination of alphabets, numbers and special characters (*, %, @, #, $, ^)

  Password age—30 days

  Account lockout after 5 attempts

  Password reuse—after 5 password changes

- Application Software Password Policy:

  Minimum 6 characters password with combination of alphabets, numbers and special characters (*, %, @, #, $, ^)

  Account lockout after 3 attempts

(b) Automatic timeout is enabled on Network devices and servers

3. Access controls

Following points are part of authorization model.

(a) A formal Change management procedure is followed to authorize and grant access on any IT system to new user.

(b) Events logs of critical devices are captured for analysis and Monitoring is done on event logs.

(c) Role based access has been defined in the application.

4. Transfer controls

Below transfer controls are in place.

(a) All Ingress/Egress Traffic (data) over public network are encrypted through SSL.

(b) Data flowing through Virtual Private Networks are secured and encrypted though IPSEC VPN model.

(c) All Ingress/Egress Traffic (data) over public network are getting logged for analysis.

(d) Authorized Gate pass/electronic copy of receipts are required well in advance for transfers of any data from IDC.

5. Input controls

Below points are implemented as part of Audit trail process.

(a) Audit trails are enabled on databases which can be further used for analysis.

(b) Events logs of critical devices are captured for analysis and Monitoring is done on event logs.

(c) Audit trails are enabled on firewall for all sets of policies.

6. Contract controls

(a) Accelya Kale is certified on ISO 9001 (quality management system) and ISO 27001 (Information security management system) and thereby follows formal procedure for contractual data.

(b) Contractor selection criterion is followed through a formal process.

(c) SLA's mentioned in contract gets monitored and reviewed at regular intervals.

7. Availability controls

Following processes are part of Data archiving

(a) Daily, weekly and monthly incremental backups are taken to avoid loss of data.

(b) 24×7×365 days of uninterrupted power supply is available at iDC.

(c) Data is protected against virus, Trojans, spywares and other malwares through host based antivirus and network based unified threat machine (@ Perimeter level).

(d) Emergency response plan is in place at iDC.

(e) Disaster recovery and Business continuity plans are in place.

8. Controls for separation of duties

(a) Duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the assets.

(b) Development, test and operational facilities are separated to reduce the risks of unauthorized access or changes to the operational system.

DATA EXPORTER	DATA IMPORTER
Name:	Name:
Authorised Signature:	Authorised Signature:

ATTACHMENT A to EU Standard Contractual Clauses for processing between IATA and Participant

EU Standard Contractual Clauses for processing between IATA and Sub-processor:

Standard Contractual Clauses (processors)

WHEREAS

(i) Pursuant to a SIS Participation Agreement between SIS Participants and International Air Transport Association ("IATA"), IATA shall provide billing and settlement services to SIS Participants which may involve the transfer of personal data to third countries for processing by IATA and its sub-processor, Accelya Kale Solutions Limited ("Accelya Kale").

(ii) For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, certain SIS Participants (as data exporters) have entered into Standard Contractual Clauses with IATA (as data importer).

(iii) Now, IATA and Accelya Kale wish to enter into these clauses to satisfy the sub-processing requirements of Clause 11 of the Standard Contractual Clauses. IATA and Accelya Kale intend these clauses to be valid as if Accelya Kale had countersigned Standard Contractual Clauses with individual SIS Participants, as envisaged by Clause 11.

Name of the data exporting organisation:

(Certain SIS Participants)

Name of the data importing organisation:

INTERNATIONAL AIR TRANSPORT ASSOCIATION
Address: 800 Place Victoria. P.O. Box 113, Montreal, Quebec, Canada, H4Z 1M1

Telefax: +1 (514) 874 1589
Tel: +1 (514) 874 0202

(the data **importer**)

And
Name of the sub-processor

ACCELYA KALE SOLUTIONS LIMITED
Address: 1st Floor Modi House, Naupada, Eastern Express Highway, Thane (W) 400 602, India

Telefax: +91 22 6780 8899
Tel: +91 22 6780 8888

(the **sub-processor**)

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

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

HAVE FURTHER AGREED that the Clauses, signed between IATA as data importer and Accelya Kale as sub-processor, shall take effect as if Accelya Kale had countersigned Standard Contractual Clauses with individual SIS Participants, as envisaged by Clause 11.

Clause 1 Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[4];

(b) *'the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the sub-processor'* means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 Details of the transfer

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

Clause 3 Third-party beneficiary clause

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

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

[4] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 Obligations of the data importer[5]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

[5] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Clause 6 Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

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

   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7 Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9 Governing Law

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

Clause 10 Variation of the contract

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

Clause 11 Sub-processing

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

Clause 12 Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

[6] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

On behalf of the data importer:

Name:	Adina Minculescu
Position:	Head, e-Invoicing Services, GDC
Address:	800 Place Victoria. P.O. Box 113, Montreal, Quebec, Canada, H4Z 1M1

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

Authorised Signature:…(Available upon Request)….

On behalf of the sub-processor:

Name:	Neela Bhattacherjee
Position:	Managing Director
Address:	1st Floor Modi House, Naupada, Eastern Express Highway, Thane (W) 400 602, India

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

Authorised Signature:…(Available upon Request)….

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

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

Sending personal data to the data importer to support and if required validate the invoices submitted for payment (using the interline billing and settlement solution provided by the data importer to the data exporter and third parties).

Data importer

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

Receiving personal data from the data exporter to support and if required validate the invoices submitted for payment (using the interline billing and settlement solution provided by the data importer to the data exporter and third parties).

Data subjects

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

Airline passengers; Crew/Staff members of the data exporter or its counterparts.

Categories of data

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

Some or all of the following: passenger name, gender, date of birth, age, frequent flyer number, contact details, payment card data (masked in accordance with Payment Card Industry Digital Security Standard (PCI-DSS) specifications) and the special categories of data listed below.

Special categories of data (if appropriate)

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

Sensitive/special personal data that is associated with a charge to the customer such as medical information (if for example a charge for oxygen applied and the personal data explicitly or implicitly referenced a medical conditions).

Processing operations

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

Personal Data to be used where required to support and validate the accuracy of charges to be billed and settled between the data exporter and third parties.

Order Control

The Data Exporter has the right to carry out an inspection at the Data Importer's office at any time. In the course of the inspection the Data Importer shall give the Data Exporter reasonable assistance including but not limited to access to any necessary information and documentation and access to premises. In particular, the Data Exporter has the right to inspect the Data Importer's compliance with all technical and organizational measures.

On behalf of the data importer:

Name:	Adina Minculescu
Position:	Head, e-Invoicing Services, GDC
Address:	800 Place Victoria. P.O. Box 113, Montreal, Quebec, Canada, H4Z 1M1

Authorised Signature:…(Available upon Request)….

On behalf of the sub-processor:

Name:	Neela Bhattacherjee
Position:	Managing Director
Address:	1st Floor Modi House, Naupada, Eastern Express Highway, Thane (W) 400 602, India

Authorised Signature:…(Available upon Request)….

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

1. Access control

Below are the access control mechanisms:

(a) Access card readers are in place at all areas of building.

(b) Access to secure areas (for e.g. access to data centre) are protected by dual authentication comprise of Biometric and access card reader

(c) Door Security is covered through access card reader along with 4 digit PIN Code.

(d) Environmental and Physical security includes CCTV surveillance cameras, Alarm Systems, Sprinklers, Smoke Detectors.

2. Accession control

Following procedures are implemented

(a) Strong Password policy is set for user authentication.

- Base System Software Password Policy:

  Minimum 8 characters password with combination of alphabets, numbers and special characters (*, %, @, #, $, ^)

  Password age—30 days

  Account lockout after 5 attempts

  Password reuse—after 5 password changes

- Application Software Password Policy:

  Minimum 6 characters password with combination of alphabets, numbers and special characters (*, %, @, #, $, ^)

  Account lockout after 3 attempts

(b) Automatic timeout is enabled on Network devices and servers

3. Access controls

Following points are part of authorization model.

(a) A formal Change management procedure is followed to authorize and grant access on any IT system to new user.

(b) Events logs of critical devices are captured for analysis and Monitoring is done on event logs.

(c) Role based access has been defined in the application.

4. Transfer controls

Below transfer controls are in place.

(a) All Ingress/Egress Traffic (data) over public network are encrypted through SSL.

(b) Data flowing through Virtual Private Networks are secured and encrypted though IPSEC VPN model.

(c) All Ingress/Egress Traffic (data) over public network are getting logged for analysis.

(d) Authorized Gate pass/electronic copy of receipts are required well in advance for transfers of any data from IDC.

5. Input controls

Below points are implemented as part of Audit trail process.

(a) Audit trails are enabled on databases which can be further used for analysis.

(b) Events logs of critical devices are captured for analysis and Monitoring is done on event logs.

(c) Audit trails are enabled on firewall for all sets of policies.

6. Contract controls

(a) Accelya Kale is certified on ISO 9001 (quality management system) and ISO 27001 (Information security management system) and thereby follows formal procedure for contractual data.

(b) Contractor selection criterion is followed through a formal process.

(c) SLA's mentioned in contract gets monitored and reviewed at regular intervals.

7. Availability controls

Following processes are part of Data archiving

(a) Daily, weekly and monthly incremental backups are taken to avoid loss of data.

(b) 24x7x365 days of uninterrupted power supply is available at iDC.

(c) Data is protected against virus, Trojans, spywares and other malwares through host based antivirus and network based unified threat machine (@ Perimeter level).

(d) Emergency response plan is in place at iDC.

(e) Disaster recovery and Business continuity plans are in place.

8. Controls for separation of duties

(a) Duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the assets.

(b) Development, test and operational facilities are separated to reduce the risks of unauthorized access or changes to the operational system.

On behalf of the data importer:

Name:	Adina Minculescu
Position:	Head, e-Invoicing Services, GDC
Address:	800 Place Victoria. P.O. Box 113, Montreal, Quebec, Canada, H4Z 1M1

Authorised Signature:…(Available upon Request)….

On behalf of the sub-processor:

Name:	Neela Bhattacherjee
Position:	Managing Director
Address:	1st Floor Modi House, Naupada, Eastern Express Highway, Thane (W) 400 602, India

Authorised Signature:…(Available upon Request)….

OPTION B: **EU Standard Contractual Clauses for processing between IATA, Participant and Sub-processor:**

Standard Contractual Clauses (processors)

WHEREAS

(i) Pursuant to an SIS Participation Agreement between SIS Participants and International Air Transport Association ("IATA"), IATA shall provide billing and settlement services to SIS Participants which may involve the transfer of personal data to third countries for processing by IATA and its sub-processor, Accelya Kale Solutions Limited ("Accelya Kale").

(ii) For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, certain SIS Participants (as data exporters) have entered into Standard Contractual Clauses with IATA (as data importer) and Accelya Kale (as sub-processor). For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation:

.....

Address:.....

.....

Tel.:.....; fax:.....; e-mail:.....

Other information needed to identify the organisation

.....

(the data **exporter**)

And

Name of the data importing organisation:

INTERNATIONAL AIR TRANSPORT ASSOCIATION
Address: 800 Place Victoria. P.O. Box 113, Montreal, Quebec, Canada, H4Z 1M1

Tel: 1 514 874 0202

(the data **importer**)

And

Name of the sub-processor:

ACCELYA KALE SOLUTIONS LIMITED
Address: "Kale Enclave", 1st floor, Sharada Arcade, Satara Road, Pune-411037, India

Telefax: +91 20 2423 1639
Tel: +91 20 6608 3777

(the **sub-processor**)

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

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

Clause 1 Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[7];

(b) *'the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the sub-processor'* means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 Details of the transfer

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

Clause 3 Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

[7] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 Obligations of the data importer[8]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

[8] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Clause 6 Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

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

   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7 Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9 Governing Law

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

Clause 10 Variation of the contract

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

Clause 11 Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses[9]. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

[9] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

On behalf of the data exporter:

Name (written out in full): _____

Position: _____

Address: _____

_____

_____

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

(Signature)

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Adina Minculescu, International Air Transport Association

Position: Head, e-Invoicing Services, GDC

Address: 800 Place Victoria, P.O. Box 113

Montréal, Québec H4Z 1M1

Canada

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

(Signature)

(stamp of organisation)

On behalf of the sub-processor:

Name (written out in full):	Neela Bhattacherjee, Accelya Kale Solutions Limited
Position:	Managing Director
Address:	1st Floor Modi House, Naupada, Eastern Express Highway
	Thane (W) 400 602
	India

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

(Signature)

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

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

Sending personal data to the data importer to support and if required validate the invoices submitted for payment (using the interline billing and settlement solution provided by the data importer to the data exporter and third parties).

Data importer

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

Receiving personal data from the data exporter to support and if required validate the invoices submitted for payment (using the interline billing and settlement solution provided by the data importer to the data exporter and third parties).

Data subjects

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

Airline passengers; Crew/Staff members of the data exporter or its counterparts.

Categories of data

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

Some or all of the following: passenger name, gender, date of birth, age, frequent flyer number, contact details, payment card data (masked in accordance with Payment Card Industry Digital Security Standard (PCI-DSS) specifications) and the special categories of data listed below.

Special categories of data (if appropriate)

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

Sensitive/special personal data that is associated with a charge to the customer such as medical information (if for example a charge for oxygen applied and the personal data explicitly or implicitly referenced a medical conditions).

Processing operations

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

Personal Data to be used where required to support and validate the accuracy of charges to be billed and settled between the data exporter and third parties.

Order Control

The Data Exporter has the right to carry out an inspection at the Data Importer's office at any time. In the course of the inspection the Data Importer shall give the Data Exporter reasonable assistance including but not limited to access to any necessary information and documentation and access to premises. In particular, the Data Exporter has the right to inspect the Data Importer's compliance with all technical and organizational measures.

DATA EXPORTER	DATA IMPORTER
Name:	Name:
Authorised Signature:	Authorised Signature:

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

1. Access control

Below are the access control mechanisms:

(a) Access card readers are in place at all areas of building.

(b) Access to secure areas (for e.g. access to data centre) are protected by dual authentication comprise of Biometric and access card reader

(c) Door Security is covered through access card reader along with 4 digit PIN Code.

(d) Environmental and Physical security includes CCTV surveillance cameras, Alarm Systems, Sprinklers, Smoke Detectors.

2. Accession control

Following procedures are implemented

(a) Strong Password policy is set for user authentication.

- Base System Software Password Policy:

  Minimum 8 characters password with combination of alphabets, numbers and special characters (*, %, @, #, $, ^)

  Password age—30 days

  Account lockout after 5 attempts

  Password reuse—after 5 password changes

- Application Software Password Policy:

  Minimum 6 characters password with combination of alphabets, numbers and special characters (*, %, @, #, $, ^)

  Account lockout after 3 attempts

(b) Automatic timeout is enabled on Network devices and servers

3. Access controls

Following points are part of authorization model.

(a) A formal Change management procedure is followed to authorize and grant access on any IT system to new user.

(b) Events logs of critical devices are captured for analysis and Monitoring is done on event logs.

(c) Role based access has been defined in the application.

4. Transfer controls

Below transfer controls are in place.

(a) All Ingress/Egress Traffic (data) over public network are encrypted through SSL.

(b) Data flowing through Virtual Private Networks are secured and encrypted though IPSEC VPN model.

(c) All Ingress/Egress Traffic (data) over public network are getting logged for analysis.

(d) Authorized Gate pass/electronic copy of receipts are required well in advance for transfers of any data from IDC.

5. Input controls

Below points are implemented as part of Audit trail process.

(a) Audit trails are enabled on databases which can be further used for analysis.

(b) Events logs of critical devices are captured for analysis and Monitoring is done on event logs.

(c) Audit trails are enabled on firewall for all sets of policies.

6. Contract controls

(a) Accelya Kale is certified on ISO 9001 (quality management system) and ISO 27001 (Information security management system) and thereby follows formal procedure for contractual data.

(b) Contractor selection criterion is followed through a formal process.

(c) SLA's mentioned in contract gets monitored and reviewed at regular intervals.

7. Availability controls

Following processes are part of Data archiving

(a) Daily, weekly and monthly incremental backups are taken to avoid loss of data.

(b) 24x7x365 days of uninterrupted power supply is available at iDC.

(c) Data is protected against virus, Trojans, spywares and other malwares through host based antivirus and network based unified threat machine (@ Perimeter level).

(d) Emergency response plan is in place at iDC.

(e) Disaster recovery and Business continuity plans are in place.

8. Controls for separation of duties

(a) Duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the assets.

(b) Development, test and operational facilities are separated to reduce the risks of unauthorized access or changes to the operational system.

DATA EXPORTER	DATA IMPORTER
Name:	Name:
Authorised Signature:	Authorised Signature: