DATA PROCESSING ADDENDUM (“ADDENDUM”)

Instruction Page

This Data Processing Addendum, including its Annexes and Appendices, (“Addendum”) forms part of the master agreement or other written or electronic agreement between Aviatrix Systems, Inc. (“Aviatrix” or “Data Processor”) and the Aviatrix customer (“Data Controller”) identified hereunder.

HOW TO EXECUTE THIS Addendum:

1. This Addendum consists of two parts: the main body of the Addendum, and Annex 1 and Annex 2 (including Appendices 1 and 2).

2. This Addendum has been pre-signed on behalf of Aviatrix. The Standard Contractual Clauses (EU Model Clause Agreement) in Annex 2 have been pre-signed by Sherry Wei, Founder and CTO Aviatrix Systems, Inc. as the data importer.

3. To complete this Addendum, Data Controller must:
   a. Complete the information in the signature box and sign on Page 8.
   b. Complete the information as the Controller or data exporter on Pages 2, 10 and 18
   c. Complete the information in the signature box and sign on Pages 16 and 19.

4. Send the completed and signed Addendum to Aviatrix by email to infosec@aviatrix.com.

Upon receipt of the validly completed Addendum by Aviatrix at this email address, this Addendum will become legally binding.

If the entity signing this Addendum is a party to the Agreement, this Addendum is an addendum to and forms part of the Agreement.

If the entity signing this Addendum is not a party to the Agreement, this Addendum is not valid and is not legally binding.

This Addendum is Between
Data Controller and Data Processor (as each are further defined in § 1) are hereinafter jointly referred to as the “Parties” and each of the Parties individually also as a “Party”.

Recitals

All capitalized terms shall have the meanings set forth herein. In the course of its business activities and under a separate commercial agreement (the “Services Agreement”), Data Processor receives from Data Controller access to certain Personal Data controlled by the Data Controller. This Addendum is concluded in order to ensure that Data Controller may meet its data protection obligations with respect to the Commissioned Processing and under Data Protection Law. This Addendum only applies to the extent that the Data Protection Legislation applies to the Processing of Personal Data under the Services Agreement, including if (a) the Processing is in the context of the activities of an establishment of either Party in the EU/EEA, and/or (b) the Personal Data relates to Data Subjects who are in the EU/EEA and the Processing relates to the offering to them of goods or services or the monitoring of their behavior in the EU/EEA by or on behalf of a Party. The Parties shall ensure that they Process Personal Data solely for the purposes contemplated in the Services Agreement or as otherwise agreed to in writing by the Parties. For the avoidance of doubt, this Addendum and the obligations hereunder do not apply to Data Processor’s use (i) of aggregated reporting or anonymized statistics; or (ii) for compliance with legal and regulatory obligations.

§ 1 Definitions

1. “Personal Data” shall mean any information relating to an identified or identifiable natural person (each a “Data Subject”). For the sake of clarity, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

2. “Commissioned Processing” shall mean Processing of Personal Data that is carried out by Data Processor on behalf of Data Controller, in accordance with the instructions of Data Controller and the terms of this Addendum.

3. “Data Protection Legislation” shall mean the General Data Protection Regulation ((EU) 2016/679) ("GDPR"), the European Directives 95/46 and 2002/58/EC (as amended by Directive 2009/136/EC) and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them (including but not limited to the Privacy and Electronic Communication (EC Directive) Regulations 2003), and all other applicable laws relating to the Processing of Personal Data and privacy that may
exist in any relevant jurisdiction, including, where applicable, the guidance and codes of practice issued by the relevant supervisory authorities).

4. “Data Subject” and “Processing” shall have the meanings given in the GDPR.

5. “EU” and “EEA” shall respectively mean the European Union and the European Economic Area.

6. “Services” shall mean the Services identified in the Services Agreement between the Parties, and as further described, for purposes of this Addendum, in § 2.1 hereof.

§ 2 Details of the Processing

1. Subject and Duration of the Services to be Carried Out

Subject and duration of the work to be carried out are set out in the Services Agreement.

2. Types of Personal Data

The following types of Personal Data and/or Personal Data categories shall be subject of the Commissioned Processing:

Name, email, address, telephone number

3. Purpose of the Commissioned Processing

Data Processor provides software support services. To the extent that through the course of performing such support services data importer receives Personal Data by access to Data exporter’s systems containing such Personal Data or receives Personal Data in log files from data exporter, data importer acts as a data processor.

4. Type and Extent of the Commissioned Processing

Data Processor shall process Personal Data only as necessary to deliver the Services according to the Services Agreement to Data Controller.

5. Categories of Data Subjects

The Data Subjects that will be impacted by the Commissioned Processing are employees, independent contractors, agents, customers and vendors of Data Controller.

6. Technical and Organizational Measures

“Technical and Organizational Measures” (as that term is defined in GDPR) to be implemented by Data Processor are stipulated in Annex 1 to this Addendum.
7. Rectification, Erasure, and Blocking of Personal Data, Portability Requests and Objection

Data Processor shall promptly (and in no event within more than three (3) business days) transmit to Data Controller any claim or request of a Data Subject arising out of the Commissioned Processing of the Personal Data by Data Processor, including but not limited to rectification, erasure, and blocking of Personal Data, portability requests, and objection. Data Processor shall not be entitled to act in its own discretion with respect to any claim or request without consultation of Data Controller.

Data Processor shall rectify, erase, and block Personal Data as ordered by Data Controller unless prohibited by law from doing so.

8. Obligations of Data Processor

Data Processor shall perform the Commissioned Processing by Processing all Personal Data only within the scope of the work to be carried out and according to documented instructions of Data Controller. Data Processor shall supervise and keep records on any technical and organizational measures with respect to § 2.6 of the Addendum on a regular basis. Data Processor shall provide Data Controller with respective records, as set forth in § 10 on request of Data Controller.

Data Processor has appointed the person listed below as a contact person for data protection purposes:

infosec@aviatrix.com

Any change in this contact person shall be disclosed promptly to Data Controller.

Data Processor shall be liable with regard to ensuring confidentiality of the Personal Data that it has received from Data Controller. All persons, including employees, officers, agents, and contractors, of Data Processor who may access the Personal Data shall be pledged in writing to confidentiality, and shall be notified of the data protection obligations specifically arising from the work to be carried out, and any order or appropriation hereof.

9. Sub-Processing

Data Controller hereby provides Data Processor with a general written authorization to employ sub-processors under this Addendum for the Commissioned Processing. Data Processor shall inform Data Controller of any intended changes concerning the addition or replacement of sub-processors, thereby giving Data Controller the opportunity to object to such changes. In the event that Data Controller objects, Data Processor shall use reasonably commercial efforts to secure another sub-processor, to which Data Controller shall also have the right to object. If Data Processor is unable to secure a satisfactory sub-processor, Data Processor shall be entitled to terminate the Services to be provided hereunder without any additional obligations to Data Controller.

Where Data Processor subcontracts its obligations under the Addendum to a sub-processor, Data Processor shall ensure that the written subcontract imposes substantially the same obligations on the sub-processor as are imposed on Data Processor under this Addendum, including compliance with § 5 hereunder.
Data Processor shall, prior to and regularly during the term of the subcontract, supervise the Technical and Organizational Measures that are necessary to protect the Personal Data and were implemented by the subcontractor. The transmission of Personal Data is only permitted if the subcontractor has implemented Technical and Organizational Measures comparable to the ones agreed upon in this Addendum and complies with the obligations in its written contract with Data Processor.

10. Rights of Data Controller to Monitor and Audit

Data Processor agrees that Data Controller is entitled to monitor its compliance with Data Protection Legislation and this Addendum during its regular business hours. Data Processor covenants to provide Data Controller with all information that is reasonably necessary to conduct these monitoring procedures within an appropriate time period, at Data Controller’s expense and subject to any confidentiality or nondisclosure agreement. If Data Controller is convinced that an audit on-site at Data Processor’s headquarters (or relevant office location(s)) is necessary, Data Processor shall allow Data Controller access to the offices of Data Processor and to the stored Personal Data and data processing programs on-site, subject to good faith negotiations between the Parties as to how and when such audit shall be carried out. Data Processor shall be entitled to put in place any confidentiality or nondisclosure agreement in order to protect its proprietary information, as well as the conditions under which such on-premise audit shall be carried out. Data Controller is entitled to have the audit carried out by a third party (auditor) that is to be appointed on an individual basis, unless the Data Processor can identify a reasonable conflict of interest with such third party, in which case Data Controller shall appoint another. Data Controller shall announce such an audit in writing at least five (5) business days in advance. Any and all monitoring and/or audit carried out by Data Controller shall be at Data Controller’s sole expense. Data Controller shall reimburse Data Processor for its reasonable expenses and time spent and incurred in connection with an audit under this section.

11. Notification of Violations of Data Processor

Data Processor shall notify Data Controller immediately about any case in which Data Processor or one of its employees breaches any provision regarding the protection of the Personal Data of Data Controller or the obligations under this Addendum.

Data Controller shall be notified about any loss, illegal transmission, or third-party acquisition of the Personal Data irrespective of causation. Data Processor shall take appropriate measures in consultation with Data Controller regarding the security of the Personal Data, as well as the reduction of possible disadvantageous consequences for the Data Subjects. Insofar as notification obligations apply to Data Controller, and to the extent applicable, and subject to the limitations in Article 28(3)(f) of the GDPR, Data Processor must assist Data Controller in fulfilling these obligations.

12. Orders by Data Controller
The Commissioned Processing of the Personal Data by Data Processor is solely carried out within the framework of the Addendum and the specific individual instructions provided by Data Controller. Data Processor shall comply with (individual) instructions regarding the type, extent and procedure of Commissioned Processing.

Data Processor shall promptly notify Data Controller if Data Processor assumes that a given instruction by Data Controller may violate Data Protection Legislation. Data Processor is entitled to suspend the Commissioned Processing of the respective instruction until it has been confirmed or amended by an authorized employee of Data Controller.

13. Erasure of Personal Data after the Commissioned Processing has been Carried Out

After the Commissioned Processing has been carried out, Data Processor shall hand over, or upon prior consent of Data Controller only, destroy in a secure and data protective manner, or safely erase according to the state of the art, all Personal Data processed for Data Controller within ninety (90) days of the termination of the Commissioned Processing hereunder. Any right of retention regarding the documentation, Personal Data, processing and utilization results and the correspondent Personal Data carrier is hereby excluded, unless (a) such Personal Data is anonymized as defined under the GDPR, in which case Data Processor shall be entitled to retain the anonymized data, or (b) EU or EU Member State law requires additional retention or storage of the Personal Data.

§ 3 Further Obligations of Data Processor

1. Data Processor shall not use the transmitted Personal Data for any other purposes than the Commissioned Processing or other than as set forth in the Recitals. Copies or duplicates must not be created without knowledge of Data Controller, provided that this is not part of the work to be carried out as set forth in this Addendum. Data Processor warrants that the Personal Data processed for Data Controller shall be held separately and segregated from any other data set.

2. Data Processor shall support Data Controller to the appropriate extent in defending against claims arising from alleged or actual violation of data protection requirements, at Data Controller’s sole expense. Data Controller shall pursue complaints issued by Data Subjects within the framework of its data protection liability to an appropriate extent and shall deal with such complaints.

3. Data Processor acknowledges that information due in response to a Data Subject’s request shall be given exclusively by Data Controller or by an authorized representative of Data Controller. To the extent that such request is impacted by the Commissioned Processing, Data Processor shall be obliged to promptly provide Data Controller with the relevant information and support Data Controller with respect to its obligations, at Data Controller’s sole expense.

4. Data Processor shall assist Data Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to Data Processor.

5. Data Processor shall notify Data Controller about the results of the inspections of any data protection supervisory authorities, to the extent that they are associated with the Commissioned Processing and this Addendum. Data Processor shall notify Data Controller about objections issued by the supervisory authorities that refer to Data Processor’s area of accountability, and shall amend ascertained objections to the extent legally required.
§ 4  Obligations of Data Controller

1. Data Controller shall be solely liable for the material legality of the Commissioned Processing, and safeguarding the rights of its Data Subjects, subject to § 6 below, including without limitation ensuring that it has provided Data Subjects with the mandated transparency associated with the Commissioned Processing under GDPR, and establishing all legal bases (and obtaining consent where consent is required) for the Processing contemplated hereunder.

2. Data Controller shall inform Data Processor of any faults, changes or irregularities (per the above paragraph regarding Data Controller’s obligations) in the Personal Data processed by Data Processor promptly upon discovery by Data Controller.

§ 5  International Transfers of Personal Data

1. With respect to any Personal Data originating from, or processed on behalf of, Data Controller within EU/EEA and transferred to Data Processor’s sub-processors within the EU/EEA, what is set out in § 2.9 regarding sub-processors shall apply hereinafter.

2. With respect to Personal Data originating from, or processed on behalf of, the Data Controller within EU/EEA, but accessed or otherwise processed by Data Processor (and/or its sub-processors) in jurisdictions outside the EU/EEA, the Parties have entered into the EU Standard Contractual Clause Agreement as set out in Annex 2 to this Addendum. The Parties agree that any disputes arising under an EU Standard Contractual Clause Agreement shall be treated as if they had arisen under the Services Agreement. Notwithstanding the foregoing, the EU Standard Contractual Clause Agreement shall not apply if the jurisdiction in which the Data Processor is established has been deemed by the EU as a jurisdiction with adequate protection for personal data or if the Data Processor and/or its sub-processors located in the U.S. has received Privacy Shield certification, provided, however, that if the EU deems Privacy Shield inadequate during the term of the Agreement and this Addendum, the Parties shall promptly ensure compliance with the EU Standard Contractual Clause Agreement as set out in Annex 2. To the extent that either Party works with a sub-processor for the Processing of the Personal Data, it shall ensure that a sub-processor complies with the EU Standard Contractual Clause Agreement included herein. The Parties further recognize that the EU governing authorities may supplement or otherwise amend any requirements that must be set forth in the EU Standard Contractual Clause Agreement under Article 46(c) of the GDPR and agree to modify the EU Standard Contractual Clause Agreement accordingly.

3. With respect to Personal Data originating from, or processed on behalf of, Data Controller outside the EU/EEA, where the Processing of Personal Data is subject to any applicable regulatory requirement (other than the Data Protection Legislation) that prohibits or restricts (i) the transfer of Personal Data to any jurisdiction, or (ii) the Processing of Personal Data in any jurisdiction (including remote access to that Personal Data from any country or territory and through the use of cloud based IT solutions), Data Processor shall not transfer or process the Personal Data in contravention of any such prohibition or restriction. In such event, the Parties shall collaborate in good faith to find a feasible solution.

§ 6  Final Provisions

1. If any of the Personal Data of Data Controller in the possession of Data Processor may be affected by seizure or confiscation, insolvency proceedings, or any other events or measures taken by a third party, Data Processor
shall inform Data Controller hereof. In addition, Data Processor shall inform any such third party that sovereignty and ownership of the Personal Data belong solely to Data Controller.

2. If one or more stipulations of this Addendum are deemed void, this shall not affect validity of the other stipulations of this Addendum. In the event of invalidity of one or more stipulations of this Addendum, the Parties shall negotiate a legally effective provision commercially close to the invalid stipulation. The same shall apply in the event of a regulatory gap. In case a change in applicable law makes an amendment of this Addendum necessary, the Parties shall discuss and agree such required change in good faith.

3. Data Controller shall indemnify Data Processor, including its subsidiaries, affiliates, officers, directors, agents, or employees, from any and all fines, sanctions, claims, losses, liabilities, damages, costs and expenses, including third-party claims, demands, reasonable attorneys’ fees, consultants’ fees and court costs (collectively, “Claims”) to the extent that such Claims arise from, or may be in any way attributable to (i) any failure by Data Controller to comply with Applicable Laws, including without limitation GDPR; (ii) any failure by Data Controller to establish proper legal bases for Processing the Personal Data that falls within the Commissioned Processing, or to properly communicate to Data Processor any changes in such legal bases (such as, without limitation, withdrawal of consent or exercise of the right to be forgotten by a Data Subject under GDPR); and (ii) the negligence, gross negligence, bad faith, or intentional or willful misconduct of Data Controller or its personnel in connection with obligations set forth herein. The Parties agree that the foregoing indemnification obligations shall (a) amend and replace any existing indemnification obligations under the Services Agreement (and any amendments thereto) with respect to the protection of Personal Data; and (b) apply irrespective of the location where such Claim is made, filed or adjudicated, whether in the United States or abroad, and irrespective of any choice of law/forum language in the Services Agreement.

4. The stipulations on choice of law and venue of jurisdiction of the Services Agreement apply to this Addendum as well.

5. In the event of any conflicting stipulations between this Addendum and other agreements in place between the Parties, the stipulations within this Addendum shall prevail.

Signed:

Place, Date

__________________________
Data Processor

Place, Date

1/18/2019

__________________________
Data Controller

Annex 1
to the Data Processing Addendum
“Technical and Organizational Measures” shall be defined as:

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymization and encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

In furtherance of the above definition, Data Processor shall take the following specific measures shall to ensure that it meets the Technical and Organizational Measures prescribed in the Addendum with respect to the Commissioned Processing:

1. **Physical access control**

Measures to prevent unauthorized persons from gaining access to data processing systems for processing or using the Personal Data:

a) Definition of persons who are granted physical access;

b) Electronic access control;

c) Issuance of access IDs;

d) Implementation of policy for external individuals;

e) Alarm device or security service outside service times;

f) Implementation of key(-card) handling policy;

h) Security doors (electronic door opener, ID reader, CCTV);

i) Implementation of measures for on-premise security (e.g. intruder alert/notification).

2. **Logical access control**
Measures to prevent that unauthorized persons use data processing equipment and procedures:

a) Password protection of personal computers.

3. **Data access control**

Measures that ensure that persons entitled to use a data processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights:

a) Implementation of partial access rights for respective data and functions;

b) Requirement of identification vis-à-vis the data processing system (e.g. via ID and authentication);

c) Implementation of policy on access- and user-roles;

d) Evaluation of protocols in case of damaging incidents.

4. **Data Transfer control**

Measures to ensure that the Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of the Personal Data by means of data transmission facilities can be established and verified.

Encryption.

5. **Entry control**

Measures to ensure that it is possible to check and ascertain whether Personal Data have been entered into, altered or removed from data processing systems and if so, by whom:

Logging of data entry.

6. **Availability control**

Measures to ensure that the Personal Data is protected against accidental destruction or loss:

a) Realization of a regular backup schedule;

b) Control of condition and respective labelling of data carriers for data backup purposes;

c) Implementation of an emergency plan;

7. **Control of data set separation**
Measures to ensure that data collected for different purposes can be processed separately.

Logical separation of data of each of Data Processor’s clients.

Annex 2

EU Model Clause Agreement

Standard Contractual Clauses (Controller to 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 organization:
Address:
Tel.: __________; fax: _______________; e-mail: ________________
Other information needed to identify the organization:

.................................................................
(the data exporter)

And

Name of the data importing organization: Aviatix Systems, Inc.

Address: 411 High St
Palo Alto, CA 94301
Tel.: ___________; fax: _______________; e-mail: infosec@aviatri.com__________________
Other information needed to identify the organization:

.................................................................
(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.
Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer’s execution of, and compliance with, the terms of these Clauses.

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; [If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words “except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data” are added.]

(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; [If these Clauses are not governed by the law of a Member State, the words "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" are deleted.]

(d) ‘the subprocessor’ means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

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; [If these Clauses are not governed by the law of a Member State, the words "within the meaning of Directive 95/46/EC" are deleted.]

(g) to forward any notification received from the data importer or any subprocessor 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 subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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

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 subprocess ing, 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

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

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

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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor 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 subprocessor, 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 subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, 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

Subprocessing

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor 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 subprocessor’s obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing 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 subprocessing 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 subprocessor 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 subprocessor 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.

On behalf of the data exporter:

[Populated with details of, and deemed signed on behalf of, the data exporter:]

Name (written out in full):
Position:
Address:

On behalf of the data importer:

Name (written out in full): Sherry Wei,

Position: Founder and CTO

Address: Aviatrix Systems, Inc.

411 High Street, Palo Alto, CA 94301

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

Signature

Sherry Wei, CTO
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:

[TO BE COMPLETED]

Data importer

The data importer is: Aviatrix Systems Inc. that provides software support services. To the extent that through the course of performing such support services data importer receives Personal Data by access to Data exporter’s systems containing such Personal Data or receives Personal Data in log files from data exporter, data importer acts as a data processor.

Data subjects

The personal data transferred concern the following categories of data subjects:

Employees, independent contractors, agents, customers and vendors

Categories of data

The personal data transferred concern the following categories of data:

<table>
<thead>
<tr>
<th>Name and Initials</th>
<th>First name / initial</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Middle name / initial</td>
</tr>
<tr>
<td></td>
<td>Last name</td>
</tr>
<tr>
<td></td>
<td>Initials</td>
</tr>
<tr>
<td>Access Credentials</td>
<td>Username</td>
</tr>
</tbody>
</table>
Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

none

Processing operations

The personal data transferred will be subject to the following basic processing activities:

Provision of support services

DATA EXPORTER

[Populated with details of, and deemed to be signed on behalf of, the data exporter:]

Name: .................................
Authorized Signature ....................

DATA IMPORTER

[Populated with details of, and deemed to be signed on behalf of, the data importer:]

Name: .................................Sherry Wei, Founder & CTO
Authorized 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):

[TO BE COMPLETED]