Juniper Networks Data Subprocessing Agreement

This subprocessing agreement (the "**Subprocessing Agreement**") is entered into by and between Juniper Networks, Inc., 1133 Innovation Way, Sunnyvale, CA 94089, United States ("**Juniper Networks"** or "**Main Processor**") and the service provider as named and described in Exhibit 2 (the "**Service Provider**" or the "**Subprocessor**") each a "**Party**", together the "**Parties**".

Preamble

WHEREAS, the Main Processor provides various services to other Juniper group companies and/or Juniper customers, the provision of which requires the transfer to and further processing of personal data by Main Processor;

WHEREAS, the Main Processor from the perspective of Applicable Data Protection Law acts as a so-called data importer or processor in relation to other Juniper group companies and/or Juniper customers (which qualify as data exporters or controllers) and has therefore concluded a data processing agreement ("**DPA**") with such Juniper group companies and/or Juniper customers (collectively, the "**Data Exporter(s)**") that incorporates the Standard Contractual Clauses as per Commission Decision 2010/87/EU of February 5, 2010 which are attached for reference purposes as Exhibit 1 to this Subprocessing Agreement ("**c2p-Model-Contract**");

WHEREAS, Subprocessor will render parts of the above-mentioned services as a subprocessor of Main Processor ("**Services**"), and under the service agreement(s) concluded by and between the Parties (the "**Contract**" or "**Contract(s)**") Subprocessor agreed to provide Main Processor with such services as described in Section 1 of Exhibit 2 (see "Processing Operations") of this Subprocessing Agreement for good and valuable consideration, the sufficiency of which is hereby acknowledged. The (i) Services and the (ii) involved transfer and further processing of personal data by Subprocessor as well as the (iii) technical and organizational security measures to be implemented and maintained by Subprocessor are described in Exhibit 2 to this Subprocessing Agreement;

WHEREAS, in rendering the Services to Main Processor, Subprocessor may from time to time collect, process (including having access to) or use information from data subjects, which may qualify as personal data or personally identifiable information (or similar terms) within the meaning of the privacy laws applicable to the Subprocessor or Data Exporter(s) ("**Personal Data**"), in particular dealing with the handling and international transfer of Personal Data ("**Applicable Data Protection Law**")

WHEREAS, from the perspective of Applicable Data Protection Law, Subprocessor's role with respect to Data Exporter(s) Personal Data is that of a subprocessor (i.e., a 1st-level-subprocessor) engaged by the Main Processor and Subprocessor agrees to receive from the Data Exporter(s), Main Processor, and/or service provider(s) Personal Data exclusively intended for processing activities to be carried out on behalf of the Data Exporter(s) in accordance with the Data Exporter's instructions, a service agreement, and a DPA between the Data Exporter(s) and the Main Processor, as described in this Subprocessing Agreement;

WHEREAS, when delegating any part of the processing activities to Subprocessor, Clause 11 of the Standard Contractual Clauses as per Commission Decision 2010/87/EU of February 5, 2010 requires Main Processor to enter into a subprocessing agreement with Subprocessor that resembles the main privacy obligations of the Standard Contractual Clauses and flows them down to the Subprocessor level to the extent that they are relevant for the activities delegated to the Subprocessor; this Subprocessing Agreement contains the terms and conditions applicable to the processing of such Personal Data by Subprocessor with the aim to ensure that Data Exporter(s), Main Processor and Subprocessor comply with Applicable Data Protection Law.

NOW, THEREFORE, the Parties agree what follows:

Clause 1
Handling of Personal Data

1. Each of the Parties will comply with the data protection laws applicable to its respective activities under this Subprocessing Agreement, including the guidance (e.g., working papers) published by the EU Article 29 Working Party. Should any (i) binding decision or order by a privacy regulator or court of competent jurisdiction or (ii) guidance by the EU Article 29 Working Party (or its successor) require changes to this Subprocessing Agreement and/or the way in which Subprocessor handles Personal Data hereunder then the Parties shall mutually implement such changes. This Subprocessing Agreement is deemed to have been concluded for each Juniper group company and/or Juniper customer that qualifies as a data exporter or controller (collectively, the "**Data Exporter(s)**") separately.

2. The terms of the c2p-Model-Contract shall apply (i) directly to the extent it addresses the Subprocessor (i.e., referred to as "sub-processor" in the c2p-Model-Contract) and (ii) analogously to the subprocessing relationship between the Parties. For the analogous application

   a) the Main Processor shall comply with Clause 3 (2) in the c2p-Model-Contract and all the obligations of the "data exporter" with the following exceptions: Clause 3 (1); Clauses 4 (a), (b) and (f) to (h) as well as Clause 8 (1) as these constitute obligations solely applicable for data exporter(s) as data controllers;

   b) the Subprocessor shall comply with the obligations of the "data importer" in the c2p-Model-Contract;

   c) the term "Member State" in the c2p-Model-Contract shall mean any country (i.e., any EU/EEA Member State or third country) in order to cover all relevant Data Exporters, regardless of their location within or outside the EU/EEA.

3. Subprocessor will implement, and maintain throughout the term of its engagement, the technical and organizational security measures described in Exhibit 2 Section 2 to this Subprocessing Agreement.

4. Upon Main Processor's request, Subprocessor shall provide a detailed description of the Services it performs as sub-processor and of the countries in which it performs such Services.

5. Subprocessor may not further delegate any of its processing activities to its own subprocessor ("2nd Level Subprocessor") in relation to the Personal Data covered hereunder, unless with the prior written permission of Main Processor. The Main Processor's written permission can be granted in the Contract. The Subprocessor shall (i) impose on any 2nd Level Subprocessors contractual obligations no less stringent than the requirements applicable to Subprocessor according to Clause 11 of Model Contract 2010/87/EU, this Subprocessing Agreement and the Contract and (ii) require that all 2nd Level Subprocessors comply with all Applicable Data Protection Laws. Subprocessor will provide copies of all such existing or new agreements with its 2nd Level Subprocessors to Main Processor upon request and without undue delay, but in any case, prior to granting 2nd Level Subprocessors access to Personal Data of the Data Exporters.

Clause 2
Compliance with local law

1. If and to the extent necessary to comply with mandatory provisions regarding the commissioning and performance of the Subprocessor under the national or local laws applicable to the Data Exporter or the Main Processor, the Main Processor may require any necessary changes (including amendments) to the provisions of this Subprocessing Agreement and its appendices. Such changes are deemed accepted by the Subprocessor if it does not reject the changes within four weeks after having received a notification of the changes in writing. The Subprocessor shall be informed about this consequence in the notification. If disputed, the necessity of a change shall be deemed proven if the Main Processor presents a respective order (which may be informal) by a competent regulator. The Main Processor is not obliged to demand that the regulator issue a formal order, or to challenge an informal order. If the Subprocessor raises objections vis-à-vis the Main Processor in writing within the four weeks period, then the Party requiring the change (i.e., the Main Processor, as the case may be) shall have the right to terminate this Subprocessing Agreement and the underlying Contract with thirty (30) days' notice in writing unless the Subprocessor chooses to continue this Subprocessing Agreement with the change.

2. The Parties agree to the amendments set out below, which are required for full compliance with mandatory requirements regarding the commissioning of Subprocessor under the national laws applicable to the Data Exporter, Main Processor and/or the Subprocessor. These amendments shall be interpreted in accordance with such national laws. Should the Data Exporter be subject to laws or regulations of a country or region which requires special processing conditions, and should these special processing conditions not be listed in Clause 2 (2), then the provisions set out in Clause 2 (2) c) below ("the GDPR Amendments") and/or Clause 2 (2) d) below ("the CCPA Amendments") shall apply mutatis mutandis. Subprocessor hereby represents that it is aware of all requirements in such national laws applicable to its provision of the Services and will at any time comply with the same even if not expressly set out in Clause 2. In addition to the foregoing, the parties shall further implement required special processing conditions upon request by Main Processor as required and applicable.

   a) **Terminology**

      For Data Exporters located outside the scope of the law of the European Union, the data protection terms used in

this Subprocessing Agreement, including the definitions set forth in the c2p-Model-Contract, shall be interpreted in accordance with the applicable local law.

b) **General processing conditions**

(i) Rectification, deletion and blocking of data: The Subprocessor shall rectify, delete and/or block Personal Data as well as perform other processing operations on Personal Data if so instructed by the Main Processor and or the Data Exporter.

(ii) Self-monitoring by the Subprocessor: The Subprocessor shall monitor, by appropriate means, its own compliance with its data protection obligations in connection with the commissioned data processing operations and shall provide the Main Processor with periodic (at least annual) and occasion-based reports regarding such controls.

(iii) Monitoring by the Data Exporter and/or Main Processor: The Data Exporter and/or Main Processor shall have the right to control, by appropriate means, the Subprocessor's compliance with its data protection obligations (in particular as regards the technical and organizational measures adopted by the Subprocessor which the Main Processor declares it has taken into consideration when entering into this agreement) annually and at any time occasion-based (e.g., by demanding information or audit reports regarding the Subprocessor's data processing systems), such controls being limited to information and data processing systems that are relevant to the Services. The foregoing also includes providing the Data Exporter and/or Main Processor with information necessary for the Main Processor to comply with applicable data privacy and security requirements. For these purposes, the Data Exporter and/or Main Processor shall also have the right to carry out on-site audits during regular business hours, without disrupting the Subprocessor's business operations and in accordance with the Subprocessor's security policies, and after a reasonable prior notice. The Subprocessor shall tolerate such audits and shall render all necessary support. Moreover, the Subprocessor commits to implement those technical and organizational security measures that are deemed necessary by the Data Exporter and/or the Main Processor; to the extent such security measures were not agreed or implied on the basis of the agreement between the Parties, the Parties shall in good faith negotiate the conditions for such additional security measures.

(iv) Notification obligation of the Subprocessor: The Subprocessor will notify the Main Processor without undue delay of (1) any suspected or actual non-compliance with statutory provisions dealing with the protection of Personal Data by the Subprocessor or its employees, and (2) any (suspected) non-compliance with the provisions of this agreement. The Subprocessor shall further notify the Main Processor, without undue delay, if it holds that an instruction violates applicable laws. Upon providing such notification, the Subprocessor shall not be obliged to follow the instruction, unless and until the Main Processor has amended the instruction or confirmed its legality. The Subprocessor shall notify the Main Processor of data subjects' complaints and requests (e.g., regarding the rectification, deletion and blocking of data) and orders by courts and competent regulators and any other exposures or threats in relation to data protection compliance identified by the Subprocessor and shall provide reasonable assistance to the Data Exporter and/ or Main Processor to respond to such complaints or requests in a timely manner. Moreover, and notwithstanding (1) and (2) above, the Subprocessor will immediately provide the Main Processor with a data breach notice if the Subprocessor becomes aware of any security incident that is likely to have impact on the availability, integrity and / or confidentiality of the Personal Data imported and/or processed by the Subprocessor (e.g., discovery of unintended data deletion, discovery of data being accessible to resources that were not or no longer authorized, discovery of unintended disclosure or data potentially having become compromised by a hacking attack or other external security threat). The data breach notice must contain as a minimum the scope of the Personal Data affected, the scope and number of data subjects affected, the time when the data breach took place, the circumstances and the effects of the data breach, the measures taken to eliminate the consequences of the breach, and any further information the Data Exporter and/or the Main Processor may require to comply with applicable national law.

(v) Right to instruction: The Data Exporter and/or Main Processor are entitled and obliged to instruct the Subprocessor in connection with commissioned data processing operations, generally or in the individual case, regarding the collection, processing and use of the data. Instructions may also relate to the correction, deletion, blocking of or any other activity performed of data. Instructions shall generally be given in writing, unless the urgency or other specific circumstances require another (e.g., oral, electronic) form. Instructions in another form than in writing shall be confirmed by the Data Exporter and/or Main Processor in writing, if the Subprocessor so requests.

(vi) Data secrecy: The Subprocessor shall ensure the confidentiality of the data processed and shall in particular not disclose the Personal Data processed to any third parties unless authorized by the Data Exporter or the Main Processor, shall process the Personal Data only for the purpose of providing the Services and shall ensure that any person acting under its authority will only process the Personal Data in accordance with the instructions of the Data Exporter and/or Main Processor. This obligation will apply also after termination of processing of the Personal Data. The Subprocessor shall be obliged to commit any person acting under its authority entrusted with the processing of Personal Data hereunder in written form to keeping any Personal Data strictly confidential and not to use such Personal Data for any other purposes except for the provision of the commissioned data processing operations and as per the Data Exporter's

and/or Main Processor's instructions to the Subprocessor. This obligation to confidentiality shall continue even after the end of the respective engagement. The Subprocessor will further instruct such persons regarding the applicable statutory provisions on data protection. The Subprocessor shall ensure that access to the data which is the subject of this agreement is limited to those persons who need access to the data to meet the Subprocessor's obligations under this agreement and only to such part or parts of the data as is strictly necessary for performance of that person's duties. Upon request, the Subprocessor will provide the Data exporter and/or Main Processor with a list of the persons having access to Personal Data with a description of their function, if any.

(vii) Data Retention / Return and further use of data after end of contract: The Subprocessor agrees and warrants not to store the Personal Data for a period longer than required by the purpose of the transfer. Upon the expiration or termination of this agreement, unless otherwise instructed by the Data Exporter and/or Main Processor, the Subprocessor shall return to the Data Exporter and/or Main Processor, without undue delay, all data carriers received from the Main Processor and all data obtained or generated in connection with the Services, including relevant copies, in whatever format, and shall refrain from any further processing and use of such data, to the extent this is possible without infringing the Subprocessor's own statutory obligations. In case of technical impossibility to return the Personal Data, the Subprocessor shall inform the Main Processor accordingly and upon request of the Main Processor delete or destroy the Personal Data. In case of technical impossibility to delete or destroy data processed in electronic form, the Subprocessor shall do whatever necessary to make said data not accessible, non-retrievable and non-modifiable and any relevant use and processing shall be prohibited. Without undue delay as of expiration or termination of this agreement, the Subprocessor shall provide the Data Exporter(s) and Main Processor with a written statement confirming it acted as per the above.

c) **Special processing conditions under the General Data Protection Regulation ("GDPR Amendments")**

(i) In order to satisfy the requirements for the commissioning of processors pursuant to Art. 28 of the Regulation (EU) 2016/679 (General Data Protection Regulation - "**GDPR**") the following amendments will apply from May 25, 2018:

(ii) Instructions: The Subprocessor will process the Personal Data only on behalf of the Data Exporter and/or Main Processor and in compliance with its instructions and the agreement, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by Union or Member State law to which the Subprocessor is subject; in such a case, the Subprocessor shall inform the Data Exporter and/or Main Processor of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Instructions shall generally be given in writing, unless the urgency or other specific circumstances require another (e.g. oral, electronic) form. Instructions in another form than in writing or in electronic form shall be documented in appropriate form. The Subprocessor shall immediately inform the Data Exporter and/or Main Processor if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

(iii) Confidentiality: The Subprocessor ensures that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(iv) Security Measures: The Subprocessor ensures that it takes and complies with all security measures required pursuant to Art. 32 GDPR.

(v) Subprocessors: For the commissioning of subprocessors by the Subprocessor, in addition to Clause 11 of the Standard Contractual Clauses 2010/87/EU, the Subprocessor shall comply with the requirements set forth in Art. 28 (2) and (4) GDPR.

(vi) Response to Data Subject requests: Taking into account the nature of the processing, the Subprocessor shall assist the Data Exporter and/or Main Processor by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Data Exporter's and Main Processor's obligation to respond to requests for exercising the data subject's rights under the GDPR.

(vii) Assistance to the Data Exporter and/or Main Processor: If so requested by the Data Exporter and/or Main Processor, the Subprocessor shall provide required assistance to the Data Exporter and/or Main Processor in ensuring its compliance with obligations pursuant to Articles 32 to 36 GDPR taking into account the nature of processing and the information available to the Subprocessor.

(viii) Return and further use of data after end of contract: After the end of the provision of services relating to the commissioned processing of Personal Data under this agreement, the Subprocessor, at the choice of the Data Exporter and/or Main Processor, shall delete or return all the Personal Data to the Data Exporter and/or Main Processor and shall delete existing copies thereof unless Union or Member State law requires storage of the Personal Data.

(ix) Monitoring by the Data Exporter and/or Main Processor: The Subprocessor shall make available to the Data Exporter and/or Main Processor all information necessary to demonstrate compliance with the obligations described in this agreement. The Data Exporter and/or Main Processor shall have the right to control, by appropriate means, the Subprocessor's compliance with its data protection obligations annually and at any time occasion-based, such controls being limited to

information and data processing systems that are relevant to the Services. For these purposes, the Data Exporter and/or Main Processor shall also have the right to carry out on-site audits, conducted by the Data Exporter and/or Main Processor or another auditor mandated by the Data Exporter and/or Main Processor, during regular business hours without disrupting the Subprocessor's business operations and in accordance with the Subprocessor's security policies, and after a reasonable prior notice. The Subprocessor shall tolerate such audits and shall render all necessary support.

d) **Special processing conditions under the California Consumer Privacy Act of 2018 ("CCPA Amendments")**

(i) No Sale of Information: Subprocessor acknowledges and confirms that it does not receive any Personal Data (which for purposes of this Clause 2 (2) d) includes "personal information" as defined under the CCPA), as consideration for any services or other items that Subprocessor provides to the Data Exporter and/or the Main Processor. Subprocessor shall not have, derive, or exercise any rights or benefits regarding Personal Data. Subprocessor must not sell any Personal Data as the term "selling" is defined in the CCPA. Also, Subprocessor must not collect, share, or use any Personal Data except as necessary to perform the Services for the Data Exporter and/or Main Processor. Subprocessor represents and warrants that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from taking any action that would cause any transfers of Personal Data to or from Subprocessor to qualify as "selling personal information" under the CCPA.

(ii) Control and Ownership: Subprocessor may not access, collect, store, retain, transfer, use, disclose or otherwise process in any manner any Personal Data, except (a) in the interest and on behalf of the Data Exporter and/or the Main Processor, and (b) as directed by authorized personnel of the Data Exporter and/or the Main Processor in writing. Without limiting the generality of the foregoing, Subprocessor may not make Personal Data accessible to any subcontractors or relocate Personal Data to new locations, except as set forth in written agreements with, or in written instructions from, the Data Exporter and/or the Main Processor. The Main Processor is not providing Subprocessor with Personal Data for any consideration for any service, and any service Subprocessor provides to the Data Exporter and/or the Main Processor is not consideration for the Main Processor providing Subprocessor with Personal Data.

(iii) Comply with Approved Policies: Subprocessor must keep Personal Data secure from unauthorized access by using Subprocessor's best efforts and state-of-the art organizational and technical safeguards. Without limitation, Subprocessor must comply with the Juniper Vendor Security Requirements and the technical and organizational security measures described in Exhibit 2 Section 2.

(iv) Assistance to the Data Exporter and/or Main Processor: At the Data Exporter and/or Main Processor's reasonable request, Subprocessor must (a) promptly provide required assistance to the Data Exporter and/or Main Processor to meet its obligations under data protection and privacy laws including providing the Data Exporter and/or Main Processor with Personal Data in a readily useable format within 30 days of a request, and (b) contractually agree to comply with laws or industry standards designed to protect Personal Data, including, without limitation, the Standard Contractual Clauses approved by the European Commission for data transfers to processors, the CCPA, PCI Standards, HIPAA requirements for business associates, as well as similar and other frameworks, if and to the extent such frameworks apply to any Personal Data that Subprocessor comes into contact with, or allow the Subprocessor shall provide required assistance to the Data Exporter and/or Main Processort to terminate certain or all contracts with Subprocessor, subject to a proportionate refund of any prepaid fees, offering transition or migration assistance as reasonably required, and without applying any early termination charges or other extra charges.

e) **General provisions regarding Clause 2 (2)**

(i) Applicability of the General Processing Conditions under the GDPR and the CCPA: Clause 2 (2) b) (i.e., the General Processing Conditions) will continue to apply under the GDPR and/or CCPA if and to the extent (1) its provisions do not contradict GDPR and/or CCPA requirements or interpretations, guidance or orders of competent authorities, or (2) are required to satisfy national implementation provisions (i.e., with respect to GDPR opening clauses) or regulations adopted pursuant to statutory authority (e.g., regulations issued by the California State Attorney General).

(ii) Order of Precedence within Clause 2 (2): In case of contradictions or inconsistencies between Clause 2 (2) b) (i.e. the General Processing Conditions) and Clause 2 (2) c) (i.e. the GDPR Amendments), Clause 2 (2) c) shall prevail. For the avoidance of doubt, provisions in Clause 2 (2) b) that merely go beyond or support provisions in Clause 2 (2) b) without contradicting Clause 2 (2) c) shall remain valid. Subsection (i) of this Clause 2 (2) e) remains unaffected.

(iii) Description of Technical and Organizational Measures: The Parties will amend Section 2 of Exhibit 2, if required, in a timely manner before the date the GDPR becomes applicable in order to meet the requirements on technical and organizational security measures as per Art. 32 GDPR.

Clause 3

Conflicts; Governing Law

1. Should there be a conflict between the c2p-Model-Contract (applicable as per Clause 1) and this Subprocessing Agreement or any other agreement between Main Processor and the Subprocessor, the c2p-Model-Contract (applicable as per Clause 1) controls.

2. If and to the extent there are contradictions or inconsistencies between Clause 2 (2) and the c2p-Model-Contract (applicable as per Clause 1), the following shall apply:

   a) If the respective Data Exporter is located in the EU/EEA and the Subprocessor is located outside the EU/EEA, the c2p-Model-Contract (applicable as per Clause 1) shall prevail. For the avoidance of doubt, in such cases the provisions in Clause 2 (2) that merely go beyond the provisions in the c2p-Model-Contract (applicable as per Clause 1), without contradicting such provisions clauses, shall remain valid.

   b) If the respective data exporter and the Subprocessor are both located in the EU/EEA, the provisions of Clause 2 (2) shall prevail.

   c) If the respective data exporter is located outside the EU/EEA, the provisions of Clause 2 (2) shall prevail.

3. The provisions in this Subprocessing Agreement shall be governed by the law of the country in which the applicable data controller (Juniper group company or Juniper customer) is established.

By signing below, each Party indicates its agreement to be bound by this Subprocessing Agreement and to incorporate the attached Exhibits 1-2, and the Juniper Vendor Security Requirements applicable to all Juniper confidential data, into this Subprocessing Agreement.

Juniper Networks, Inc.
by

Name: Meredith McKenzie_____

Position: VP, Deputy General Counsel__

Date: _____

Signature: _____

[*Insert name of Subprocessor*]
by

Name: _____

Position: _____

Date: _____

Signature: _____

Exhibit 1 to the Subprocessing Agreement
(c2p-Model Contract)

Standard Contractual Clauses for 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 organisation: [...]
(the data exporter)

And

Name of the data importing organisation: [...]
(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.

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;

(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. 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 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 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

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 subprocessing, 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 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.

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
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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. 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 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 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.

On behalf of the data exporter: [...]

On behalf of the data importer: [...]

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):
see Section 1 of Exhibit 2

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
see Section 1 of Exhibit 2

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):
see Section 1 of Exhibit 2

Categories of data

The personal data transferred concern the following categories of data (please specify):
see Section 1 of Exhibit 2

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):
see Section 1 of Exhibit 2

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):
see Section 1 of Exhibit 2

DATA EXPORTER

Name: …
Authorised Signature …

DATA IMPORTER

Name: …
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):

See Section 2 of Exhibit 2

Exhibit 2 - Details of the transfer and description of the processing and technical and organizational security measures
(Service Description)

Section 1 - Details of the transfer and description of the processing
Main Processor

The Main Processor is Juniper Networks, Inc. (as the data importer vis-à-vis the Juniper group companies and/or Juniper customers as data exporter(s)). Where the Main Processor is the data importer for Juniper group companies, the Main Processor offers and operates certain services and processes Personal Data including: (i) information or material in Juniper managed systems, databases and applications, as well as Juniper systems, databases, or applications externally managed by authorized cloud operators of the Juniper Network group companies; and (ii) information or materials shared with and received from employees, prospective employees, and other personnel of the Juniper Networks group companies. Where the Main Processor is the data importer for Juniper customer data, the Main Processor provides the following services and processes Personal Data relating to such services: technology infrastructure management and information security management including but not limited to operating systems, remote access appliance, and software-defined networking services.

Subprocessor

The Subprocessor is *[Supplier, please insert name of your entity and provide a description of your business/services]*.

Data Subjects

Please identify the groups of people whose data you may receive or process.

- *Employees*
- *Contractors*
- *Candidates*
- *Customers*
- *Business Partners*

Please delete from the above list if any of the types of data subjects listed are not relevant or add to the list as needed.

Categories of Personal Data

Please identify only the categories of data you will receive or process. Please delete from the following list if any of the types of data listed will not be transferred, or add to the list as needed.

- *names*
- *addresses, and other contact details*
- *phone number*
- *email*
- *age and/or date of birth*
- *gender*
- *National Identification Number (e.g., SSN)*
- *family and social circumstances such as marital status or dependent details*
- *education and training details, which may include academic records, qualifications, skills, training records, professional expertise, and/or work Experience*
- *financial details such as bank account information or details, and information pertaining to salary, bonus, and/or equity*

Please add any other types of information/data that identifies a data subject (i.e. other categories of data that may

be considered personally identifiable information or personal data), or remove from above if not applicable.

Special Categories of Data (if appropriate)

The Personal Data transferred concern the following Special Categories of Data:

*(*Special Categories of Data may include personal data relating to race, ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, health, or sexual orientation. Supplier, please list the Special Categories of Data you will process, or put "N/A" or "Not Applicable" if you will not transfer or process any such types of data.)*

Processing Operations

The services to be provided by Subprocessor under the Contract shall be:

[Supplier, please provide a description of the services to be supplied pursuant to the contract]

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

[Supplier, please provide a description of how data will actually be processed]

Section 2 - Technical and organizational measures

INTRODUCTION

This document describes the technical and organizational measures and processes that the Subprocessor, shall, as a minimum, implement and maintain in order to protect Personal Data against risks inherent in the Processing and all unlawful forms of Processing, including but not limited to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed. Subprocessor shall keep any necessary written records and documentation (including in electronic form) to evidence its compliance with these technical and organizational security measures and shall make them immediately available to Juniper Networks on request.

The security measures described in this document apply without prejudice to any other specific statutory requirements for technical and organizational measures that may be applicable.

Subprocessor will at any time comply with the specific statutory requirements for technical and organizational security measures stipulated in the national law applicable to the data exporter. Subprocessor hereby represents that it is aware of such specific statutory requirements and has implemented the necessary security measures even if they are not expressly detailed in the following.

1. DEFINITIONS

a) Incident or Security Incident: Any event or set of events that indicates an attack upon, unauthorized use of, or attempt to compromise computing or networking systems that may lead to a Data Breach.
b) Internal Systems: Devices that perform computing or networking services to provide or support Subprocessor's Services.
c) Information Systems: Information technology resources providing services that transmit, process, handle, store, modify, or make available for access Personal Data.
d) Data Breach: Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
e) Strong Authentication: Means the use of authentication mechanisms and authentication methodologies stronger than passwords as herein. Strong Authentication methods could include one-time passwords, multi-factor authentication, or digital certificates with passphrases on the private key.

2. SYSTEM SECURITY

a) Access Controls. Subprocessor shall implement and maintain the following access controls to prevent any unlawful form of Processing (including but not limited to unauthorized use, access or disclosure of Personal Data) and Data Breaches.
   i. Unique user IDs must be assigned to all individual users.
   ii. Procedures for timely access removal must be implemented and regularly assessed.
   iii. The principles of least privilege and need to know must be implemented and followed.
   iv. The principles of least privilege and need to know must be regularly reviewed on a periodic basis (e.g. regular account and access reviews).
   v. Passwords:
      (1) All passwords have the following attributes:
         - Minimum length of 8 characters.
         - Complexity must be at least three of the following four criteria (i) one uppercase letter, (ii) one lowercase letter, (iii) one number, (iv) one special character.
         - Changed at least once every ninety (90) days.
         - Passwords cannot be any of the five (5) previous passwords.
         - Initial or temporary passwords are changed after first use.
         - Default passwords are changed upon deployment.
         - Passwords are never sent in clear text format.
         - Passwords are not shared amongst users.
      (2) Authentication:
         - Authentication credentials are protected by encryption during transmission.
         - Login attempts are limited to no more than five (5) consecutive failed attempts with user account being locked out for at least five (5) minutes upon reaching such limit.
         - Remote administration access, by the Subprocessor, to the Subprocessor's Information Systems that can access Personal Data shall use two (2) factor authentication.

(3) Sessions:

- Must automatically terminate sessions or activate a password-protected screensaver when user sessions are inactive for fifteen (15) minutes.
- Management systems such as jump stations or bastion hosts must time out sessions at regular intervals, not to exceed twelve (12) hours.

b) Scanning and Administration. Subprocessor implements the following controls to maintain the security and integrity of Information Systems utilized in Processing Personal Data.

i. Subprossessor shall use industry security resources (e.g., National Vulnerability Database "NVD", CERT/CC Advisories) to monitor for security alerts.
ii. Subproccessor shall receive security advisories from their third party vendors.
iii. Internal and external facing systems must be regularly scanned with industry standard security vulnerability scanning software to identify security vulnerabilities.
iv. Discovered vulnerabilities must be remediated as follows a) Critical vulnerabilities within seven (7) days, b) High vulnerabilities within fourteen (14) days, c) Medium vulnerabilities within thirty (30) days, and d) Low vulnerabilities as necessary based on risk impact to Information Systems.
v. Information Systems must have appropriate security hardening (e.g. CIS benchmarks) applied before deployment and maintained thereafter.
vi. Systems and applications must log security events.
vii. Logs must provide sufficient details as required in an investigation of events.
viii. Logs must be maintained for a minimum of twelve (12) months.
ix. Logs must be monitored on a regular basis.
x. A patch management program must be maintained to ensure up-to-date security patches are appropriately applied to Information Systems.
xi. Anti-malware controls must be implemented and signature based tools must check for new updates at least daily.
xii. A formal, documented change control process must be implemented for Information Systems.

3. NETWORK SECURITY

a) Network. Subprocessor implements and maintains network security measures including the following.

i. Subprocessor's WiFi must be secured using secure encryption protocols.
ii. Firewalls must implement a default deny methodology.
iii. A DMZ must be implemented to separate backend systems from Internet facing systems.
iv. A three-tier architecture must separate database systems from web application servers.
v. Changes to the network must be sufficiently tested.
vi. An intrusion detection or prevention system must be implemented that covers network traffic to the Information Systems.
(1) The events and alerts generated must be regularly reviewed.

4. END USER DEVICES

a) Laptops and desktops used by Subprocessor personnel that may come into contact with Personal Data must meet the following requirements:

i. Full-disk encryption implemented.

b) Smartphones and Tablets must not be allowed to access, process, or store Personal Data.
c) Bring Your Own Device (BYOD)

i. If allowed at all on Subprocessor's premises or network, Subprocessor must have a published policy regarding their use.
ii. BYOD or personally-owned devices must not be allowed to access, process, or store Personal Data as well as administer Information Systems that have Personal Data.

5. INFORMATION AND DATA SECURITY

a) Information Security Policy

i. Subprocessor must implement an Information Security Policy that is reviewed at least annually.
ii. Subprocesor must have an Information Security Policy that is approved by the CISO, CIO or appropriate executive.
iii. Subprocessor shall ensure that all employees, contractors, and subcontractors with access to Personal Data are familiar and comply with the Information Security Policy.
iv. Subcontractors must comply with the requirements outlined in this document.

b) Data protection requirements

i. Transport
   (1) Encrypt the transfer of Personal Data, including backups, over external networks.
   (2) Encrypt Personal Data when transferred via physical media.
ii. Storage
   (1) Encrypt Personal Data, including backups, at rest.
iii. Business Continuity
   (1) A documented business continuity policy.
iv. Backup and Recovery
   (1) Subprocessor must have documented backup procedures.
   (2) Subprocessor must have a documented and tested disaster recovery plan.
v. Retention, Destruction and Return
   (1) Retention as permitted or required by law.
   (2) Have a documented policy for retention, destruction, or return of Personal Data.
   (3) Provide for secure erasure or certification of destruction at the end of the media's lifecycle, for media used to store Personal Data.
vi. Job Control
   (1) Implement suitable measures to ensure that, in the case of commissioned processing of Personal Data, the Personal Data are processed strictly in accordance with the instructions of the Main Processor. This shall be accomplished as follows:
      - Measures are implemented to ensure that Main Processor's instructions regarding processing of Personal Data will be followed and brought to the attention of the staff dealing with the processing of Personal Data;
      - Main Processor will be granted regular access and control rights upon request as more closely defined in the services agreement signed between Juniper Networks and the Subprocessor; and
vii. Separation of processing for different purposes
   (1) Implement suitable measures to make sure that data collected for different purposes can be processed separately. This shall be accomplished as follows:
      - access to Personal Data is separated through application security for the appropriate users;
      - within the database, Personal Data is adequately protected to ensure it is only available to applicable authorized persons;
      - interfaces, batch processes, and reports is designed for only specific purposes and functions, so data collected for specific purposes is processed separately.
viii. Customer separation
   (1) Logical and/or physical separation of Personal Data from Subprocessor's other customers' data and Personal Data processed for different purposes.
ix. Classification
   (1) Personal Data is classified as such and appropriate handling practices are documented.
x. Third parties
   (1) Third parties are granted access to Personal Data only upon Main Processor's and/or data exporter's express prior written permission for each single case or as permitted under the services agreement signed between Juniper Networks and the Subprocessor (e.g., as regards commissioning of subcontractors).

6. INCIDENT RESPONSE

a) Plan and Point of Contact:
   i. A documented incident response plan must be maintained.
   ii. A helpline or e-mail contact must be provided for employees or contractors to report security incidents.
   iii. Determine if an incident has resulted in a Data Breach or is reasonably suspected to have resulted in a Data Breach and take immediate actions to mitigate it.
b) Data Breach notification.
   i. Notification to Juniper of a Data Breach must occur without undue delay and no later than twenty-four (24) hours after becoming aware of it.
   ii. Data Breach notification must include:
      (1) What happened and how many records are involved.
      (2) The measures and mitigation steps taken or planned to be taken to address the Data Breach.
      (3) The name and contact details for more information about the Data Breach.

7. SECURE DEVELOPMENT

Subprocessors must implement and follow controls associated with the development, pre-production testing and delivery of any and all Services provided to Juniper. For this section, Software or Hardware means the

result of development, design, installation, configuration, production, or manufacture of computing code or device that supports or implements the Services. These secure development practices shall include the following:

a) Development requirements.
   i. Develop, implement, and comply with industry-standard secure coding best practices.
   ii. Follow industry-standard best practices to mitigate and protect against known and reasonably predictable security vulnerabilities, including but not limited to:
      (1) unauthorized access
      (2) unauthorized changes to system configurations or data
      (3) disruption, degradation, or denial of service
      (4) unauthorized escalation of user privilege
      (5) service fraud
      (6) improper disclosure of Juniper data
   iii. Separate test and stage environments from the production environment.
   iv. Non-production systems must not contain production data.
   v. Scan source code for security vulnerabilities prior to release to production.
   vi. Test applications for security vulnerabilities prior to release to production.

b) Open source and third party software.
   i. Industry-standard processes must be implemented to ensure that any open-source or third party software included in Subprocessor's software or hardware does not undermine the security posture of the Subprocessor or Juniper Networks.

8. AUDITS OR ASSESSMENTS

a) Subprocessor security audits or assessments.
   i. Must be performed at least annually.
   ii. Must be performed against the ISO 27001 standard, SOC2 standard or other equivalent, alternative standards.
   iii. Must be performed by a reputable, independent third party at Subprocessor's selection and expense.
   iv. Must result in the generation of an audit report or certification that will be made available to Juniper Networks on request.
   v. An annual penetration test must be performed by a third party.

9. TRAINING

a) Security and privacy training.
   i. Information security and privacy training or awareness communications must be provided to all personnel with access to Personal Data upon hire and subsequently at least once per year. The content should include but not be limited to company and policy requirements, security risks, and user responsibilities.

10. PHYSICAL SECURITY

a) Program and facilities.
   i. A physical security program must be maintained in accordance with industry standards and best practices.
   ii. Only secure data center facilities must be used to store Personal Data, including those with SSAE 16 or similar reports.

Further measures implemented by the Subprocessor:

*Please indicate any security measures the Subprocessor has implemented **in addition** to the above described measures:*

Juniper Vendor Security Requirements

INTRODUCTION

This document describes measures and processes that the Vendor shall, at a minimum, implement and maintain in order to protect all Juniper Networks confidential data, including Personal Data (collectively, "Juniper Data"), against risks inherent in the Processing and all unlawful forms of Processing, including but not limited to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Juniper Data transmitted, stored or otherwise processed. Vendor shall keep any necessary written records and documentation (including in electronic form) to demonstrate its compliance with these technical and organizational security measures and shall make them immediately available to Juniper Networks on request.

The security measures described in this document apply without prejudice to any other specific statutory requirements for technical and organizational measures that may be applicable.

DEFINITIONS

a) Information Systems: Information technology resources that transmit, process, handle, store, modify, or make available for access, Juniper Networks information and provide services as a part of this agreement.
b) Incident or Security Incident: Any event or set of events that indicates an attack upon, unauthorized use of, or attempt to compromise computing or networking systems that may lead to a Data Breach.
c) Data Breach: Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Juniper Data transmitted, stored or otherwise processed.

1. SYSTEM SECURITY

a) Access controls.
   i. Unique IDs must be assigned to all individual users.
   ii. Procedures for timely access removal must be implemented and regularly assessed.
   iii. The principles of least privilege and need to know must be implemented and followed.
   iv. The principles of least privilege and need to know must be regularly reviewed on a periodic basis (e.g. regular account and access reviews).
   v. Passwords:
      (1) Passwords must be a minimum of 8 characters in length.
      (2) Password complexity must contain at least three of the following four criteria: (i) one uppercase letter, (ii) one lowercase letter, (iii) one number, and (iv) one special character.
      (3) Passwords must be changed at least once every ninety (90) days.
      (4) Passwords cannot be any of the five (5) previous passwords.
      (5) Initial or temporary passwords must be changed after first use.
      (6) Default passwords must be changed upon deployment.
      (7) Passwords must never be sent in clear text format.
      (8) Passwords must not be shared amongst users.
   vi. Authentication:
      (1) Authentication credentials must be protected by encryption during transmission.
      (2) Login attempts must be limited to no more than five (5) consecutive failed attempts with the account being locked out for at least five (5) minutes upon reaching the limit.
      (3) Remote administration access, by the Supplier, to the Supplier's Information Systems that can access Juniper data shall use two (2) factor authentication.
   vii. Sessions:
      (1) A password-protected screensaver must be activated when user sessions are inactive for fifteen (15) minutes.
      (2) Management systems, such as jump stations or bastion hosts, must time out sessions at regular intervals not to exceed twelve (12) hours.
b) Scanning and administration.
   i. Industry security resources (e.g., National Vulnerability Database "NVD", CERT/CC Advisories) must be monitored for security alerts.
   ii. Supplier must receive security advisories from their third party vendors.
   iii. Internal and external facing systems must be regularly scanned with industry standard security vulnerability scanning software to identify security vulnerabilities.

iv. Discovered vulnerabilities must be remediated as follows a) Critical vulnerabilities within seven (7) days, b) High vulnerabilities within fourteen (14) days, c) Medium vulnerabilities within thirty (30) days, and d) Low vulnerabilities as necessary based on risk impact to Information Systems.
v. Information Systems must have appropriate security hardening (e.g. CIS benchmarks) applied before deployment and maintained thereafter.
vi. Systems and applications must log security events.
vii. Logs must provide sufficient details as required in an investigation of events.
viii. Logs must be maintained for a minimum of twelve (12) months.
ix. Logs must be monitored on a regular basis.
x. A patch management program must be maintained to ensure up-to-date security patches are appropriately applied to Information Systems.
xi. Anti-malware controls must be implemented and signature based tools must check for new updates at least daily.
xii. A formal, documented change control process must be implemented for Information Systems.

2. NETWORK SECURITY

a) Network.
i. Wi-Fi must be secured using secure encryption protocols.
ii. Firewalls must implement a default deny methodology.
iii. A DMZ must be implemented to separate backend systems from Internet facing systems.
iv. A three-tier architecture must separate database systems from web application servers.
v. Changes to the network must be sufficiently tested.
vi. An intrusion detection or prevention system must be implemented that covers network traffic to the Information Systems.
(1) The events and alerts generated must be regularly reviewed.

3. END USER DEVICES

a) Laptops and desktops.
i. Full-disk encryption must be implemented.
b) Smartphones and tablets.
ii. Smartphones and tablets must not be allowed to access, process, or store Juniper data.
c) Bring Your Own Device (BYOD).
i. If allowed on Supplier's premise or network, Supplier must have a published policy regarding their use.
ii. BYOD or personally owned devices must not be allowed to access, process, or store Juniper data as well as administer Information Systems that have Juniper data.

4. INFORMATION AND DATA SECURITY

a) Information Security Policy.
i. An Information Security Policy must be implemented and reviewed on an at least an annual basis.
ii. The Information Security Policy must be approved by the CISO, CIO, or appropriate executive.
iii. All employees, contractors, and subcontractors with access to Juniper data must agree to comply with the Information Security Policy.
iv. Subcontractors must comply with the requirements outlined in this document.
b) Data protection requirements.
i. Transport
(1) Encrypt the transfer of Juniper data, including backups, over external networks.
(2) Encrypt Juniper data when transferred via physical media.
ii. Storage
(1) Encrypt Juniper data, including backups, at rest.
iii. Business Continuity
(1) A documented business continuity plan must be implemented.
iv. Backup and Recovery
(1) Documented backup procedures must be implemented.
(2) A documented and tested disaster recovery plan must be implemented.
v. Retention, Erasure, Destruction and Return
(1) A documented policy for retention, secure erasure, destruction or return of Juniper data must be implemented.
(2) Information assets containing Juniper data must be either destroyed or securely erased at the end of their lifecycle.

vi. Separation of processing for different purposes
    (1) Where necessary to ensure Juniper data is only available to authorized persons, implement measures to make sure that data collected for different purposes can be processed separately.
vii. Customer separation
    (1) Juniper data must be logically or physically separated from the data of other customers.
viii. Classification
    (1) A classification policy and handling practices must be documented to protect Juniper data.
ix. Third parties
    (1) Third parties may only be granted access to Juniper data upon Juniper Networks' permission for each single case or as permitted under the services agreement signed between Juniper Networks and the Supplier (e.g., as regards commissioning of subcontractors).

5. INCIDENT RESPONSE

a) Plan and point of contact.
   i. A documented incident response plan must be maintained.
   ii. A helpline or e-mail contact must be provided for employees or contractors to report security incidents.
   iii. Determine if an incident has resulted in a Data Breach or is reasonably suspected to have resulted in a Data Breach and take immediate actions to mitigate it.
b) Data Breach notification.
   i. Notification to Juniper of a Data Breach must occur without undue delay and no later than twenty-four (24) hours after becoming aware of it.
   ii. Data Breach notification must include:
      (1) What happened and how many records are involved.
      (2) The measures and mitigation steps taken or planned to be taken to address the Data Breach.
      (3) The name and contact details for more information about the Data Breach.

6. SECURE DEVELOPMENT

a) Development requirements.
   i. Develop, implement, and comply with industry-standard secure coding best practices.
   ii. Follow industry-standard best practices to mitigate and protect against known and reasonably predictable security vulnerabilities, including but not limited to:
      (1) unauthorized access
      (2) unauthorized changes to system configurations or data
      (3) disruption, degradation, or denial of service
      (4) unauthorized escalation of user privilege
      (5) service fraud
      (6) improper disclosure of Juniper data
   iii. Separate test and stage environments from the production environment.
   iv. Non-production systems must not contain production data.
   v. Scan source code for security vulnerabilities prior to release to production.
   vi. Test applications for security vulnerabilities prior to release to production.
b) Open source and third party software.
   i. Industry-standard processes must be implemented to ensure that any open-source or third party software included in Supplier's software or hardware does not undermine the security posture of the Supplier or Juniper Networks.

7. AUDITS OR ASSESSMENTS

a) Supplier security audits or assessments.
   i. Must be performed at least annually.
   ii. Must be performed against the ISO 27001 standard, SOC2 standard or other equivalent, alternative standards.
   iii. Must be performed by a reputable, independent third party at Supplier's selection and expense.
   iv. Must result in the generation of an audit report or certification that will be made available to Juniper Networks on request.
   v. An annual penetration test must be performed by a third party.

8. TRAINING

a) Security and privacy training.

i. Information security and privacy training or awareness communications must be provided to all personnel with access to Juniper data upon hire and at least once per year. The content should include but not be limited to company and policy requirements, security risks, and user responsibilities.

9. PHYSICAL SECURITY

a) Program and facilities.
   i. A physical security program must be maintained in accordance with industry standards and best practices.
   ii. Only secure data center facilities must be used to store Juniper data, including those with SSAE 16 or similar reports.

Further measures implemented by the Supplier:
*Please indicate any security measures the Supplier has implemented **in addition** to the above described measures:*