Juniper Networks Data Protection Agreement
Suppliers/Subprocessors

This Juniper Networks Data Protection Agreement (the "Data Protection Agreement" or "DPA") is entered into by and between Juniper Networks, Inc., 1133 Innovation Way, Sunnyvale, CA 94089, United States ("Juniper Networks") and the supplier named below (the "Supplier"). Supplier has been engaged to provide products and/or services (the "Products and Services") to Juniper Networks and/or any of its direct and indirect affiliates in accordance with a master agreement (the "Contract").

Juniper Networks and Supplier agree as follows:

1. **Definitions**. Terms used in this DPA shall have the meaning indicated below unless otherwise defined in this DPA or in applicable laws or regulations.

   1.1 "*Data Protection Requirements*" shall mean any laws, regulations, statutes, directives, orders, rules, or contractual requirements related to the Processing of Juniper Data by the Supplier or by the Products and Services;

   1.2 "*Juniper*" shall mean Juniper Networks and any of its affiliates to whom the Supplier provides the Products and Services;

   1.3 "*Juniper Data*" shall mean any Personal Data and any Confidential Information (as such term is defined in the Contract or applicable law) of Juniper and any Juniper employees, contractors, customers, or partners that is Processed by Supplier or the Products and Services;

   1.4 "*Personal Data*" shall mean (i) any information or data that alone or together with any other data or information relates to an identified or identifiable natural person and (ii) any other information or data considered to be personally identifiable information, personal data or personal information under applicable law.

   1.4 "*Processing*" shall mean any operation or set of operations performed on data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2. **Processing Solely for Juniper; No Sale of Personal Data**: Supplier will Process Juniper Data only on behalf of Juniper and in compliance with Juniper Network's written instructions, the Contract and this DPA. If additional Processing is required by applicable Data Protection Requirements, Supplier shall inform Juniper Networks of the applicable requirement in writing before such Processing (to the extent permitted by applicable law). No Personal Data is Processed by Supplier as consideration for any products or services provided to Juniper Networks. Supplier is prohibited from "selling" any Personal Data of Juniper, as the term "sell" or its equivalent is defined in applicable Data Protection Requirements. To the extent that any Personal Data of any California consumer is included in the Juniper Data, Supplier provides the certification under the California Consumer Privacy Act ("CCPA") attached as Exhibit 4 hereto.

3. **Compliance with applicable Data Protection Requirements:** Supplier agrees to comply with the Data Protection Requirements applicable to the Processing of Juniper Data by Supplier and by the Products and Services under the Contract and this DPA. Supplier shall inform Juniper Networks if, in its opinion, an instruction from Juniper Networks would violate applicable Data Protection Requirements. .

4. **Subprocessors:** Juniper Networks' grants its general advance written permission for Supplier to delegate Processing to subprocessors ("Subprocessors"), subject to this DPA and Exhibit 1. Supplier shall impose

on any Subprocessors contractual obligations no less stringent than the requirements applicable to Supplier under the Contract and this DPA..

5. **Monitoring**: Upon written request of Juniper Networks, Supplier shall provide a report (together with any underlying materials referenced therein) to Juniper Networks regarding its compliance with Data Protection Requirements applicable to Supplier's Processing of Juniper Data and the Products and Services and this DPA. Juniper Networks shall also have the right to carry out on-site audits during regular business hours, without disrupting Supplier's business operations and in accordance with Supplier's reasonable and written security policies, and after reasonable prior notice.

6. **Data Secrecy**: Supplier shall protect the confidentiality of Juniper Data Processed and shall not disclose Juniper Data to any third parties unless authorized by Juniper Networks. Supplier shall limit access to Juniper Data to those persons who need access to meet the Supplier's obligations under this DPA and the Contract. Supplier shall ensure that all persons who Process Juniper Data for Supplier have appropriate written or legal confidentiality obligations. Data secrecy requirements shall continue even after expiration or termination of this DPA and/or the Contract.

7. **Security Measures**: Supplier shall ensure that it complies with all security measures required pursuant to applicable Data Protection Requirements, the Contract and this DPA, including the Security Requirements and Technical and Organizational Measures described in Exhibit 3, and with any data protection measures that Supplier identified in responses to any Juniper Networks vendor on-boarding questionnaires. Suppliers of Products and Services that Juniper or its partners resell or distribute to customers shall also comply with any specific security requirements identified by Juniper Networks in any written notice to Supplier as being applicable to such Products or Services.

8. **Security Incident Notifications**: Supplier will notify Juniper Networks in writing promptly and in no event later than the time period required under any applicable Data Protection Requirements, of any data breach or security incident that is likely to have an impact on the availability, integrity and/or confidentiality of the Juniper Data Processed by the Supplier or the Products and Services. Such notice must contain as a minimum the scope of the Juniper 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 Juniper Networks may require to comply with applicable national law.

9. **Cooperation**: Supplier shall notify Juniper Networks of data subject requests regarding any Personal Data included in the Juniper Data and, upon request by Juniper Networks, shall provide reasonable assistance to Juniper Networks in responding to such inquiries or requests in a timely manner. Upon request, Supplier shall promptly provide reasonably appropriate assistance with obligations under applicable Data Protection Requirements such as audits, assessments, inspections, data protection impact assessments, notifications of security incidents and consultations with legal and regulatory authorities.

10. **Data Export:** Upon Juniper Networks' written request, Supplier shall provide a list of the countries in which it Processes any Juniper Data. To the extent required under applicable Data Protection Requirements, Processing of any Personal Data of Juniper by Supplier will be subject to the Standard Contractual Clauses as per European Commission Decision 2010/87/EU of February 5, 2010 which are incorporated by reference into this DPA ("c2p-Model-Contract") and Exhibits 1 and 2, or other mechanism applicable under such Data Protection Requirements. In the event of any conflict between the c2p-Model-Contract and this DPA or any other agreement between Juniper Networks and the Supplier, the c2p-Model-Contract shall control to the extent required under applicable Data Protection Requirements.

11. **Data Retention**: Supplier shall not store Juniper Data for a period longer than required by the purpose of the Contract. Upon the expiration or termination of this DPA or the Contract, and unless otherwise instructed by Juniper Networks, Supplier shall securely return to Juniper Networks or destroy, without undue delay, all Juniper Data in any format, unless and solely to the extent that retention is required under applicable law.

Supplier shall provide Juniper Networks with a written confirmation of such return or destruction.

12. **Conflicts**. In case of a conflict between applicable Data Protection Requirements and any of the provisions of this DPA related to any Personal Data that is Processed under the Contract, then such Data Protection Requirements shall apply and prevail solely with respect to the relevant Personal Data, and solely to the extent necessary to resolve such conflict with this DPA.

By signing below, each party indicates its agreement to be bound by this DPA, including Exhibits 1-4.

* * * *Signature Page Follows* * * *

Juniper Networks, Inc. by

Lily Fang, Senior Director, Chief Privacy & Information Security Counsel

Date: March 19, 2020

Signature: DocuSigned by: Lily Fang EAB1A3D20743427...

SUPPLIER: _____

by

Name: _____

Position: _____

Date: _____

Signature: _____

EXHIBITS:

Exhibit 1	c2p-Model-Contract Appendices and Details Of Transfer
Exhibit 2	Juniper Networks as Data Processor
Exhibit 3	Security Requirements and Technical and Organizational Measures
Exhibit 4	California Consumer Privacy Act (CCPA) Certification

Exhibit 1
c2p-Model-Contract Appendices and
Details Of Transfer

Appendix 1 to c2p-Model-Contract and Details of Transfer

Data Exporter

The Data Exporter is Juniper Networks, Inc. (which may be the data importer vis-à-vis the Juniper Networks group companies and/or Juniper Networks customers as data exporter(s), as set forth in Exhibit 2). Where the Data Exporter is the data importer for Juniper Networks group companies as set forth in Exhibit 2, Data Exporter offers and operates certain services and processes Personal Data including: (i) information or material in Juniper Networks-managed systems, databases and applications, as well as Juniper Networks systems, databases, or applications externally managed by authorized third parties of the Juniper Networks 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 Data Exporter is the data importer for Juniper Networks customer data as set forth in Exhibit 2, Data Exporter 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. Further details regarding Data Exporter's activities as a data importer for Juniper Networks group companies are set forth in Exhibit 2. The DPA is deemed to have been concluded for each Juniper Networks group company and/or Juniper Networks customer or partner on behalf of whom Juniper Networks processes Juniper Data (collectively, the "Data Exporter(s)") separately.

Data Importer

The Data Importer is Supplier.

Data Subjects

Suppliers of operational/administrative products and services may Process data related to the following individuals.

- Juniper Personnel (including employees, contractors, interns, and other temporary workers)
- Recruiting-Related Individuals (including candidates and individuals acting as references)
- Juniper Customers (including their employees, contractors, interns, other temporary workers, and other users)
- Juniper Business Partners (including partners, suppliers, and other vendors)

Suppliers of products and services that Juniper resells or otherwise distributes to customers or partners may also Process Personal Data identified in the applicable Contract as well as in any specifications or documentation for the products or services.

Categories of Personal Data

The Personal Data Processed may include the following categories of data:

- Personal Contact Information (including name, and personal addresses, phone numbers, and email addresses)
- Work Contact Information (including work addresses, phone numbers, and email addresses)
- Detailed Personal Information (including age and/or date of birth, gender, marital status, photos, former names, emergency contact information, and dependent information)
- National Identification Number (e.g., social security number, social insurance number, driving license number, student number, national ID card number, and passport number)
- Education and Skills Information (including education history, degrees earned, institutions attended, academic records, qualifications, skills, training details, training records, professional expertise, work history and experience, and other resume/CV information)
- Financial Information (including bank account information or details, information pertaining to salary, bonus, equity, taxes, benefits, credit, credit cards, and expenses)

If Supplier provides products and services that Juniper resells or otherwise distributes to customers or partners, the categories of Personal Data may also include any data identified in the applicable Contract as well as in any specifications or documentation for the products or services.

Special Categories of Data (if appropriate)

The Personal Data concerns the following Special Categories of Data:

None unless expressly identified in the Contract.

Processing Operations and Subject Matter of Processing

The Products and Services set forth in the Contract.

Duration of Processing

Supplier shall process Personal Data for the duration set forth in the Contract solely in order to perform the Services, and in accordance with the DPA.

The Personal Data will be subject to the following basic processing activities

The processing activities required in order to fulfill Supplier's obligations to provide the Products and perform the Services as set forth in the Contract.

Supplemental Information

Additional information regarding the data processing may be available in the "Supplemental Privacy Information" section of Data Exporter's Privacy Policy, which is available at https://www.juniper.net/us/en/privacy-policy/.

Additional Requirements

Supplier shall comply with industry standards for data protection applicable to the Personal Data that is Processed by Supplier or by the Products of Services, including the current PCI DSS requirements and any Network Advertising Initiative , the Digital Advertising Alliance, the European Advertising Standards Alliance or other marketing-related self-regulatory frameworks and codes in the United States and other regions globally, to the extent applicable to the Personal Data that is Processed by Supplier or the Products and Services.

To the extent that new or modified provisions are required under applicable Data Protection Requirements for specific jurisdictions or geographic areas, such as data export provisions or data localization provisions, the parties agree that such provisions may be provided as necessary to Supplier (such as through the Juniper Supplier Center or the Juniper Privacy Policy (https://www.juniper.net/us/en/privacy-policy/)) and are automatically incorporated herein as of their effective date solely to the extent they are required and solely to the extent they are applicable to Juniper Data Processed by Supplier or by the Products and Services.

Subprocessors

Except as set forth in the DPA and this Exhibit 1, Supplier may not further delegate any of its Processing to any subprocessor without the prior written permission of Juniper Networks.

To the extent required under applicable Data Protection Requirements, Supplier shall inform Juniper Networks of any intended changes concerning the addition or replacement of any Subprocessors.

Upon written request, Supplier shall provide to Juniper Networks a complete list of Subprocessors that Process any Personal Data to give Juniper Networks the opportunity to object to any such Subprocessors.

Prior express written approval of Juniper Networks is required for any Subprocessors that are (a) banned from providing products or services to the United States government or any other government in the applicable territory covered by the Contract or (b) listed on the United States Department of The Treasury SDN List available at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

Appendix 2 to c2p-Model-Contract

Description of the technical and organizational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached): See Exhibit 3.

Exhibit 2 – Juniper Networks as Data Processor

This Exhibit 2 includes additional provisions regarding a Juniper Networks affiliate's or subsidiary's activities as a data importer on behalf of another Juniper Networks affiliate or subsidiary or a Juniper Networks customer. In such a case, the Juniper Networks affiliate or subsidiary is the main data importer and data processor of Personal Data ("Main Processor") and Juniper Networks or the Juniper Networks customer (as applicable) acts as a data exporter and data controller.

1. The Main Processor has concluded a Data Processing Agreement with such Juniper group companies and/or Juniper customers (collectively, the "Data Exporter(s)" for purposes of this Exhibit 2) that incorporates the c2p-Model-Contract and the relevant Appendices attached as Exhibit 1.

2. Supplier may render parts of the above-mentioned services as a subprocessor of Main Processor under the Contract. The (i) Services and (ii) involved transfer and further Processing of Personal Data by Supplier as well as the (iii) technical and organizational security measures to be implemented and maintained by Supplier are described in Exhibits 1 and 3 to this Data Protection Agreement and shall comply with Article 32 of Regulation (EU) 2016/679 General Data Protection Regulation ("GDPR").

3. In rendering the Services to Main Processor, Supplier may from time to time collect, Process (including having access to) or use information from data subjects, which may qualify as Personal Data within the meaning of the applicable Data Protection Requirements.

4. When Supplier acts as a subprocessor, it shall Process Personal Data in accordance with the Data Exporter's instructions, the Contract, and the DPA.

5. The terms of the c2p-Model-Contract shall apply (i) directly to the extent it addresses the Supplier (i.e., referred to as "sub-processor" in the c2p-Model-Contract) and (ii) analogously to the data processing relationship between the Supplier and the Main Processor. 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 as these constitute obligations solely applicable for data exporter(s) as data controllers;

    b. the Supplier shall comply with the obligations of the "data importer" in the c2p-Model-Contract; and

    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.

Exhibit 3 – Security Requirements and Technical and Organizational Measures

INTRODUCTION

This document describes the technical and organizational measures and processes that the Supplier, shall, at a minimum, implement and maintain in order to protect Juniper Data (as defined in the DPA) 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. Supplier 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 Data Protection Requirements for technical and organizational measures that may be applicable to Supplier or the Products and Services.

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 Supplier's Services.
c) Information Systems: Information technology resources providing services that transmit, process, handle, store, modify, or make available for access Juniper Data and provide Services pursuant to the Contract.
d) Juniper Systems: devices and information technology resources owned, operated, or otherwise made available to Supplier by Juniper that transmit, process, handle, store, modify, or make available for access Juniper Data.
e) Data Breach: 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.
f) Strong Authentication: 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. Supplier 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 Juniper 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 12 characters.
         - Complexity must include at least three of the following four criteria (i) one uppercase letter, (ii) one lowercase letter, (iii) one number, and (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 must be changed after first use.
- Default passwords must be changed upon deployment.
- Passwords must never sent in clear text format.
- Passwords must not be shared amongst users.

(2) Authentication:

- Authentication credentials must be protected by encryption during transmission.
- Login attempts must be 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 Supplier, to the Supplier's Information Systems that can access Juniper 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. Supplier implements the following controls to maintain the security and integrity of Information Systems utilized in Processing Juniper Data.

i. Supplier shall use industry security resources (e.g., National Vulnerability Database "NVD", CERT/CC Advisories) to monitor for security alerts.
ii. Supplier 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. Supplier implements and maintains network security measures including the following.

i. Supplier'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 Supplier personnel that may come into contact with Juniper Data must meet the following requirements:

i. Full-disk encryption must be implemented.

b) 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 premises 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.

5. INFORMATION AND DATA SECURITY

a) Information Security Policy
   i. Supplier must implement an Information Security Policy that is reviewed at least annually.
   ii. Subprocessor must have an Information Security Policy that is approved by the CISO, CIO or appropriate executive.
   iii. In the event Supplier accesses Juniper Systems, whether to process Juniper Data or for any other reason, Supplier shall comply with Juniper's then-current Information Security Policy.
   iv. In the event Supplier processes Juniper Data using its Information Systems, Internal Systems, or other Supplier resources, Supplier shall implement and maintain the controls and practices set forth in this Exhibit.
   v. Supplier's Subprocessors and other subcontractors must comply with the requirements outlined in this Exhibit.

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 documented and implemented, and must be tested at least annually.
   iv. Backup and Recovery
      (1) Supplier must have documented and implemented backup procedures.
      (2) Supplier must have a documented disaster recovery plan that is tested at least annually.
   v. Retention, Erasure, Destruction and Return
      (1) Supplier may retain Juniper Data only as required by Data Protection Requirements.
      (2) Have a documented and implemented policy for retention, secure erasure, destruction, or return of Juniper Data.
      (3) Information assets containing Juniper Data must be either destroyed or securely erased at the end of their lifecycle..
   vi. Job Control
      (1) Implement suitable measures to ensure that, in the case of commissioned processing of Juniper Data, the Juniper Data are processed strictly in accordance with the instructions of Juniper Networks. This shall be accomplished as follows:
         - Measures are implemented to ensure that Juniper Networks' instructions regarding processing of Juniper Data will be followed and brought to the attention of the staff dealing with the processing of Juniper Data;
         - Juniper Networks will be granted regular access and control rights upon request as more closely defined in the Contract; and
   vii. Separation of processing for different purposes
      (1) To ensure Juniper Data is only available to authorized persons, implement suitable measures to separately process data collected for different purposes. This shall be accomplished as follows:
         - access to Juniper Data is separated through application security for the appropriate users;
         - within the database, Juniper 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
      Juniper Data must be logically or physically separated from Supplier data of its other customers.
   ix. Data Classification

(1) A data classification policy and handling practices policy must be documented and implemented to protect Juniper Data.

x. Third parties
   (1) Third parties may only be granted access to Juniper Data only upon Juniper Networks' express prior written permission for each case or as permitted under the Contract (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 and tested at least annually.
   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

Supplier must implement and follow controls associated with the development, pre-production testing and delivery of any and all Services provided to Juniper Networks. For this section, Software or Hardware means the result of development, design, installation, configuration, production, or manufacture of computing code or devices that support or implement 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 Supplier's software or hardware does not undermine the security posture of the Supplier or Juniper Networks.

8. 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.

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 Juniper 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 Juniper Data, including those with SSAE 18 for data centers that process Juniper Data that includes financial information, or AT 101 for data centers that process other Juniper Data, or similar reports.

Exhibit 4 – CCPA Certification

To the extent that Supplier Processes any personal information of any consumer covered by the California Consumer Privacy Act, Cal. Civil Code Sec. 1798-100 et seq. ("**CCPA**") under the Contract and this DPA, Supplier confirms it is acting as a service provider to Juniper (as such terms "personal information," "consumer" and "service provider" are defined in the CCPA).

Except as otherwise required by applicable laws or regulations, Supplier is prohibited from:

(i) "selling" (as such term is defined in the CCPA) personal information in connection with the processing of personal information included in the Juniper Data under the Contract;

(ii) retaining, using or disclosing personal information included in the Juniper Data received by Supplier under the Contract for any purpose other than:

(1) providing products or services to Juniper under the Contract;
(2) retaining and employing another service provider as a subcontractor;
(3) for internal use in building products or services or improving the quality of products or services;
(4) detecting data security incidents, or protecting against fraudulent or illegal activity; or
(5) purposes enumerated in Civil Code section 1798.145, subsections (a)(1) through (a)(4).

and

(iii) retaining, using or disclosing such personal information outside of the direct business relationship between Juniper Networks and Supplier.

Pursuant to the CCPA, Supplier certifies that it understands these restrictions and will comply with them with respect to any personal information of any consumer covered by the CCPA that is processed by Supplier under the Contract.