SUPPLIER DATA PROTECTION AGREEMENT

This Supplier Data Protection Agreement ("DPA") is effective as of the date of the last signature ("Effective Date") and is entered into by and between Juniper Networks, Inc. on behalf of itself and any of its Affiliates to whom the Supplier provides the Products and Services ("Juniper") and the supplier ("Supplier") named in a Master Services Agreement or other contract ("Contract") under which Supplier has been engaged to provide products and/or services ("Products and Services") to Juniper. This DPA is incorporated into the Contract and applies to Supplier's Processing of Juniper Data.

Juniper 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.

   a. *"Affiliate"* means a company controlling, controlled by, or under common control with Juniper Networks, Inc.

   b. "Data Protection Requirements" shall mean any laws, regulations, statutes, directives, orders, or rules related to the Processing of Personal Data by the Supplier or by the Products and Services.

   c. "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.

   d. "Personal Data," "Data Subject," "Supervisory Authority," "Process," "Processor," "Sell," "Share," "Service Provider," and "Controller" will each have the meaning given to them (or their similar terms) in applicable Data Protection Requirements. "Personal Data" as used herein specifically refers to Personal Data processed by Supplier on Juniper's behalf in connection with the Contract.

   e. "Personal Data Breach" has the meaning given to it (or its similar terms) by Data Protection Requirements and includes security incidents that are likely to have an impact on the availability, integrity and/or confidentiality of Personal Data Processed by Supplier or the Products and Services.

   f. "Standard Contractual Clauses" means: (i) the Standard Contractual Clauses annexed to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 or any subsequent version thereof released by the European Commission (which will automatically apply) (the "EU SCCs"); (ii) where UK Data Protection Requirements (as defined in Section 12(d)) applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("UK Addendum").

2. **General Processing Terms**: As between Juniper and Supplier, and if applicable under Data Protection Requirements, Juniper is the Controller of Personal Data and Supplier is a Processor or Service Provider of that data. If Juniper is a Processor, Supplier is a Subprocessor (defined in Section 6). Supplier will Process Personal Data only on behalf of Juniper and in compliance with Juniper's written instructions, the Contract and this DPA. Juniper may issue additional instructions in writing. If Supplier determines that additional Processing is required by applicable Data Protection Requirements, Supplier shall inform Juniper 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.

3. **Additional US Privacy Obligations**: To the extent that Supplier Processes Personal Data that is subject to applicable US Data Protection Requirements, then Supplier: (i) shall not Sell or Share Personal Data; (ii) shall Process Personal Data only to provide the Products and Services and shall not Process Personal Data for any other purpose, except as may be permitted by applicable Data Protection Requirements; (iii) shall not Process Personal Data collected by Supplier outside of the direct business relationship between the parties, except as may be permitted by applicable Data Protection Requirements; (iv) shall not combine Personal Data received from Juniper pursuant to this Agreement with Personal Data that Supplier receives from or on behalf of another person(s), except as required to provide the Products and Services; and (v) grants Juniper the right, upon notice, to take reasonable and appropriate

steps to stop and remediate Supplier's unauthorized use of Personal Data as permitted by applicable Data Protection Requirements.

4. **Compliance with applicable Data Protection Requirements**: Supplier agrees to comply with the Data Protection Requirements applicable to the Processing of Personal Data by Supplier and by the Products and Services under the Contract and this DPA, including provision of any legally required notices to Data Subjects. Supplier shall promptly notify Juniper if it determines that it can no longer meet its obligations under Data Protection Requirements. If in Supplier's opinion, an instruction from Juniper would violate applicable Data Protection Requirements or if Supplier is unable to comply with Data Protection Requirements or this DPA, Supplier shall (i) promptly inform Juniper of such infringement or of its inability to comply with Juniper's instructions, providing a reasonable level of detail as to the instructions with which it cannot comply and the reasons why it cannot comply, to the greatest extent permitted by applicable law, and (ii) Process (or continue to Process) Personal Data to the extent Supplier is able to comply with Juniper's instructions in order to provide the Products and Services as set forth in the Contract.

5. **Compliance with U.S. Bulk Sensitive Data Rule, Executive Order 14117.** This section applies with respect to any Access to Juniper's or its customers' U.S. Bulk Sensitive Personal Data or Government-Related Data ("Covered Data") by a Country of Concern or Covered Person, including any Covered Data Transaction, as each term is defined in the Final Rule implementing Executive Order 14117 issued by the U.S. Department of Justice. Supplier represents, warrants, and covenants that: (a) Supplier, its Affiliates, employees, and contractors who have Access to Covered Data are not Covered Persons; (b) Supplier and its Affiliates will not engage in any Covered Data Transaction; and (c) Supplier will immediately notify Juniper in writing if any of the foregoing in this section changes or is no longer true.

6. **Subprocessors:**
   a. Juniper grants its general advance written permission for Supplier to delegate Processing to other processors ("Subprocessors"). Supplier shall provide Juniper a list of its Subprocessors upon request or provide Juniper with a link to a published list of Subprocessors. Supplier shall impose on any Subprocessors contractual obligations no less stringent than the requirements applicable to Supplier under the Contract and this DPA as well as any terms required to be included under applicable Data Protection Requirements, and if Subprocessors further delegate their own obligations to additional third parties, Supplier shall require its Subprocessors to impose the same restrictions on such third parties. Upon Juniper's written request, Supplier shall promptly provide to Juniper copies of the data protection, data privacy, and information security terms it has in place with its Subprocessors, provided Supplier may redact confidential terms unrelated to the foregoing. Third parties engaged by Supplier shall be deemed the Subprocessors of Supplier and shall not be the employees, contractors, or Subprocessors of Juniper. Supplier shall be fully liable for the actions of its Subprocessors as if performed by Supplier itself.

   b. To the extent required under applicable Data Protection Requirements, Supplier shall inform Juniper of any intended changes concerning the addition or replacement of any Subprocessors, and Juniper shall have the opportunity to object to any such Subprocessors. If the Parties are unable to resolve an objection based on a reasonable belief that the Subprocessor would be unable to comply with the requirements of this DPA, Juniper may terminate the Contract and receive a refund of any unused prepaid fees and shall be entitled to any other rights it has under the Contract.

   c. Notwithstanding the provisions of Section 6(a), prior express written approval of Juniper 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.

7. **Monitoring**: Upon Juniper's written request, Supplier shall provide a report (together with any underlying materials referenced therein) to Juniper regarding its compliance with Data Protection Requirements and this DPA, including access logs to Personal Data. Juniper shall also have the right to carry out on-site audits during regular business hours, without disrupting Supplier's business operations, in accordance with Supplier's reasonable and written security policies provided to Juniper, and after reasonable prior notice. Supplier shall promptly resolve any noncompliance with this DPA or Data Protection Requirements at its expense.

8. Data Secrecy:

a. Supplier shall protect the confidentiality of Personal Data it Processes and shall not disclose Personal Data to any third parties unless authorized by Juniper. Supplier shall limit access to Personal 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 Personal Data for Supplier are subject to appropriate written or legal confidentiality obligations. Data secrecy requirements shall continue even after expiration or termination of this DPA and/or the Contract.

b. Supplier shall, to the extent permitted by applicable law, (i) promptly notify Juniper of any binding law enforcement, judicial, or government request or order for Personal Data, including from a Supervisory Authority, ("Government Request") and (ii) provide Juniper with all relevant information and assistance regarding the request, without responding to such request, unless otherwise required by applicable law (including to provide acknowledgement of receipt of the request). Whether or not Supplier is legally permitted to inform Juniper of the Government Request, Supplier will establish internal policies, reporting channels, and procedures for handling Government Requests, and will consult with legal and other advisors to thoroughly evaluate and scrutinize any Government Request and seek to appropriately narrow or challenge requests which, among other reasons, are not necessary and proportionate, violate Data Protection Requirements in other jurisdictions, or are otherwise legally insufficient. When challenging a Government Request, Supplier shall seek (or, as applicable, provide Juniper reasonable assistance in seeking) interim measures to suspend the effects of the Government Request until an applicable court or other authority has decided on the merits. If the Government Request does conflict with Data Protection Requirements in other jurisdictions, including the SCCs or other data transfer mechanism, Supplier shall so inform the government agency. Supplier shall not disclose Personal Data requested until required to do so under applicable law. Supplier shall disclose Personal Data under a Government Request only to a government agency with appropriate authority under applicable law to demand the information. In responding to the Government Request, Supplier shall only provide the minimum amount of Personal Data necessary based on a reasonable interpretation of the Government Request. Supplier will document its actions and maintain a record of its assessments and handling of each Government Request. Upon request, Supplier will provide Juniper with such records relevant to Personal Data except as prohibited by applicable law. Supplier will notify its applicable Supervisory Authority to seek feedback regarding complying with the Government Request if applicable law prohibits Supplier from notifying Juniper regarding the Government Request.

9. Security Measures: Pursuant to Data Protection Requirements, the Contract, and this DPA, and taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Supplier will implement appropriate technical and organizational measures to protect against Personal Data Breaches. Such measures shall include the Security Requirements and Technical and Organizational Measures described in Exhibit 2. Supplier shall regularly test, assess and evaluate the effectiveness of the measures. 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 in any written notice to Supplier as being applicable to such Products or Services.

10. Security Incident Notifications:

a. Supplier will notify Juniper in writing promptly and in no event later than the time period required under any applicable Data Protection Requirements of any Personal Data Breach. Such notice must contain at a minimum the scope of the Personal Data affected, the scope and number of Data Subjects affected, the time when the Personal Data Breach took place, the circumstances and the effects of the Personal Data Breach, the measures taken to eliminate or mitigate its consequences, and any further information Juniper may require to comply with applicable law. Juniper may, at its election, and in coordination Supplier, take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data.

b. Supplier shall make no announcements, statements, or press releases, or publish (or have published) any other material regarding an actual or suspected Personal Data Breach where such materials identify Juniper without Juniper's prior written approval. Supplier shall assist Juniper in good faith within the timeframes for Juniper to provide Personal Data Breach notifications to finalize the content of any notifications to Data Subjects or regulatory authorities.

11. Cooperation:

a. Supplier shall notify Juniper of any request, inquiry, or complaint from Data Subjects regarding Personal Data ("Data Subject Inquiry"), and upon request by Juniper, shall provide reasonable assistance to Juniper in responding to Data Subject Inquiries in a timely manner and in any event within a timeframe providing Juniper sufficient time to respond as set forth in Data Protection Requirements.

b. 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, documentation, and consultations with legal and regulatory authorities.

12. Data Export:

a. Upon Juniper's written request, Supplier shall provide a list of the countries in which it Processes any Personal Data. Supplier shall comply with Exhibit 3 in its processing of Personal Data outside of the country from which the Personal Data originated.

b. If Supplier transfers the Personal Data, either directly or via onward transfer, of Data Subjects from located in one jurisdiction to another jurisdiction which the Data Protection Requirements in such originating jurisdiction concluded does not provide an adequate level of protection for such Personal Data, such transfer shall be subject to the protections and provisions of the Standard Contractual Clauses or other binding and appropriate transfer mechanisms that provide an adequate level of protection in compliance with Data Protection Requirements. Where the transfer mechanism is the Standard Contractual Clauses, the applicable terms of the Standard Contractual Clauses are incorporated herein by reference.

c. If the applicable transfer mechanism is the EU SCCs, Juniper shall be deemed to have signed the EU SCCs in Exhibit 1, Annex I, in its capacity of "data exporter" and Supplier in its capacity as "data importer." Module Two or Module Three of the SCC shall apply to the transfer depending on whether Juniper is Controller of the Personal Data (for Module Two) or a Processor of the Personal Data on behalf of a Controller (for Module Three). With regards to optional clauses within the EU SCCs, Clause 7 is not selected and the optional paragraph within Clause 11 is not selected. If Module Three applies, Juniper hereby notifies Supplier that it is a Processor and the instructions shall be as set forth in Section 2. For purposes of Clauses 17 and 18 of the EU SCCs, the Parties select The Netherlands.

d. Where Personal Data originating from the United Kingdom is processed by Supplier outside of the United Kingdom, in a country that has not been designated by the UK Information Commissioner's Office as ensuring an adequate level of protection pursuant to Data Protection Requirements, and to the extent such processing and transfer would be subject to the Data Protection Requirements applicable in the United Kingdom ("UK Data Protection Requirements") the Parties agree that: (i) the EU SCCs shall also apply to the processing of such Juniper Data, subject to the UK Addendum, which is completed as follows: (i) Table 1 and 2 of the UK Addendum completed with the information within Exhibit 1, attached hereto, and in accordance with the information set forth withins Section 12(c) and 6(a), (ii) Table 3 is completed with the information within Exhibit 1 and Exhibit 2 and (iii) and the option "neither party" is selected in Table 4.

e. For Personal Data originating from Switzerland, references in the EU SCCs to: (i) the words "EU" and "EEA" are replaced with the "Switzerland"; (ii) "EU Data Protection Law" is replaced with "Federal Act on Data Protection"; and (iii) the "European Commission" is be replaced with the "Federal Data Protection and Information Commissioner". The term "member state" is interpreted to include data subjects in Switzerland.

f. Supplier shall apply the data protection principles of accountability and data minimization to any cross-border transfers of Personal Data, such that it regularly assesses the access controls set forth in Exhibit 2 that it implements and the extent of Personal Data in its possession prior to any transfer, and that it limits Personal Data transferred across borders to that which is strictly necessary to provide the Services.

g. In the event of any conflict between the Standard Contractual Clauses and this DPA or any other agreement between Juniper and the Supplier, the Standard Contractual Clauses shall control to the extent required under applicable Data Protection Requirements and to the extent of the conflict. The Standard Contractual Clauses will cease to apply if Supplier has implemented an alternative and legally-compliant data transfer mechanism for the lawful transfer of personal data in accordance with applicable Data Protection Requirements and has notified Juniper of its use of such data transfer mechanism.

13. **Data Retention**: Supplier shall not store Personal 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, Supplier shall securely return to Juniper or destroy, without undue delay, all Personal Data in any format, unless and solely to the extent that retention is required under applicable law, and in the event of such required retention, Supplier warrants it will continue to protect such Personal Data in accordance with this DPA, will cease use of the data, and will retain the data only for so long as required by such applicable law. Supplier shall provide Juniper with a written confirmation of such return or destruction upon request.

14. **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.

IN WITNESS WHEREOF, the parties have entered into this the Supplier Data Protection Agreement as of the Effective Date.

Juniper Networks, Inc.		**Supplier:** ___________________________	
By:	Signed by: Laura Flier 34636739390E481...	By:	
Name:	Laura Flier	Name	
Title:	Corporate Attorney, Sr. Manager Privacy	Title:	
Date:	May 2, 2025	Date:	

Juniper Networks
Legal Department
Laura Flier
Approved As To Form
Laura Flier

EXHIBIT 1
APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

ANNEX 1

A. LIST OF PARTIES

Data Exporter

Name: Juniper Networks, Inc. (which may be the data importer vis-à-vis its applicable Affiliates)
Address: as set forth in the Contract.
Contact person: To the attention of Legal Privacy if by mail or to privacy@juniper.net if sent electronically.
Activities relevant to the data transferred under these Clauses: as set forth in the Contract.
Signature and date: refer to DPA.
Role: Controller, except when Processing data on behalf of its customers or other Data Exporter Affiliates, in which case data exporter is a Processor.

Data Importer

Name: The Data Importer is Supplier.
Address: as set forth in the Contract.
Contact person: as set forth in the Notices provision in the Contract.
Activities relevant to the data transferred under these Clauses: as set forth in the Contract.
Signature and date: refer to DPA.
Role: Processor, or sub-processor if Data Exporter is a Processor.

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose personal data is transferred:

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 transferred:

The Personal Data transferred 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.

Sensitive Categories of Data (if appropriate): None unless expressly identified in the Contract.

The frequency of the transfer: As set forth in the Contract.

Nature of the Processing: For Supplier to provide the Products and Services set forth in the Contract.

Purposes of the data transfer and further Processing: The Processing activities defined in the DPA and in the Contract.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Supplier shall retain Personal Data for the duration set forth in the Contract solely in order to perform and provide the Products and Services, and in accordance with the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: As set forth in the DPA and in the Contract.

C. COMPETENT SUPERVISORY AUTHORITY

The Netherlands.

ANNEX II

Technical and organizational measures including technical and organizational measures to ensure the security of the data:

See Exhibit 2 to the DPA.

ANNEX III

List of Supplier Subprocessors:

Refer to Section 6 in the DPA.

EXHIBIT 2 – 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 take account of the risks involved in the Processing, the nature of the Personal Data, and the nature, scope, context, and purposes of Processing in assessing the necessary level of security. 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 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: Any 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. Compliance with below Juniper *Third Party Secure Access* guidelines for applicable access methods:

(1) Juniper Managed Device (Juniper-issued laptop)

- Juniper-laptop will be imaged and installed with Juniper's standard tools
- Role-based access provisioning and control
- Disabled administrative privileges or privilege elevation

(2) Juniper's Desktop as a Service Virtual Desktop Infrastructure (VDI) Solution

- Administrative access on the computer to install the VDI client with vendor IT support
- Installation of Amazon WorkSpaces client or a Tehama Personal Computer over Internet Protocol (PCoIP) client on third-party device with vendor IT support

(3) VPN Access Using Vendor's Own Device

- Full Disk Encryption (FDE) via Microsoft Bitlocker or Apple FileVault
- Minimum Operating System versions: Microsoft Windows 10 or MacOS 10.12 patched within one month
- Minimum Operating System versions for Mobile Devices: iOS 14.8 or Android 8.0 MDM enrolled
- Approved Anti-Virus (AV) and/or Anti-Spyware product

vi. 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 be 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.

(4) Credential Sharing:

- Mechanisms must exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.

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, CISA's KEV Catalog) 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.

xiii. Clock synchronization of all networked systems using trusted protocols like NTP/PTP for correlation and analysis of security-related events and other recorded data

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.
      (2) Periodically test ability to temporarily isolate critical sub-networks if the network is under attack

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) Refer section 2.a.v. of this document for Third Party Secure Access guidelines.
d) 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 requirements.
   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.
      (3) Monitor, detect and block the disclosure of sensitive information via different channels (email, cloud, removable media, file transfer, mobile devices, etc.) with data leakage prevention measures/tool that is reviewed/updated at least once annually.
   ii. Storage
      (1) Encrypt Juniper Data, including backups, at rest.
   iii. Encryption Requirements
      (1) Strong encryption is used for all encryption of at least 256 bits.
      (2) Encryption keys are reliably managed.
   iv. Pseudonymization
      (1) Where possible, Juniper Data shall be pseudonymized such that Juniper Data cannot be attributed to a particular individual without use of additional information.
      (2) Pseudonymization may include hashing, randomizing, obfuscating, truncating, tokenizing, and removing identifiers.
      (3) The additional information needed to attribute the pseudonymized Juniper Data to an individual must be held in

separate repositories by Supplier and subject to strict security measures to prevent combination of the information with the pseudonymized Juniper Data.

v. Business Continuity
   (1) A documented business continuity plan must be documented and implemented and must be tested at least annually.
   (2) Redundancy of information processing facilities via (i) Using geographically separate data centers with mirrored systems, and duplicate components in systems (CPU, hard disks, memories) and networks (firewalls, routers, switches); and (ii) mechanisms in place to alert organization and Juniper to any failure in information processing facilities (+ establish out-of-band communication channel).

vi. 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.

vii. Retention, Erasure, Destruction and Return
   (1) Supplier may retain Juniper Data only as required by Data Protection Requirements or other applicable laws, or for so long as the data are needed to provide the Products and Services under the Contract.
   (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.

viii. 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 Juniper's instructions. This shall be accomplished as follows:
      - Measures are implemented to ensure that Juniper's instructions regarding processing of Juniper Data will be followed and brought to the attention of the staff dealing with the processing of Juniper Data.
      - If set forth in the Contract, Juniper will be granted regular access and control rights upon request.

ix. 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.

x. Customer separation

   Juniper Data must be logically or physically separated from Supplier data of its other customers.

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

xii. Third parties
   (1) Third parties may only be granted access to Juniper Data only upon Juniper's 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.
   iv. Document relevant facts related to the Data Breach and keep a record of such facts.

b) Data Breach notification.
   i. Notification to Juniper of a Data Breach must occur without undue delay and no later than seventy-two

(72) hours after becoming aware of it.

ii. Data Breach notification must include:

(1) The scope of the Juniper Data affected, the scope and number of individuals affected, the time when the Data Breach took place, the circumstances and the effects of the Data Breach, the measures taken to eliminate or mitigate its consequences, and any further information Juniper may require to comply with applicable law.

(2) The name and contact details to obtain 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. 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.

vii. Exclude from Software and Hardware and ensure no code used on or in connection with Software or Hardware constitute or may be used as backdoors or other similar code allowing access to Internal Systems, Juniper Systems, or Juniper Data. Supplier shall not change its business processes that would facilitate access to Internal Systems, Juniper Systems, or Juniper Data. Supplier represents and warrants that no laws or government policies applicable to Supplier require the creation of backdoors, facilitation of such access, or provision of encryption keys to government authorities.

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.

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 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 3 – ADDITIONAL PROVISIONS
BASED ON EUROPEAN DATA PROTECTION BOARD RECOMMENDATIONS 01/2020

1. Supplier shall provide, upon Juniper's reasonable written request, logs regarding access to Personal Data.
2. Supplier's legal and audit personnel are provided information regarding applicable transfers of Personal Data prior to the transferring of any such data, where such information may include an explanation of the necessity of the transfer and any data protection safeguards in scope.
3. In the event Supplier receives a request to voluntarily disclose unencrypted Personal Data to a government authority, Supplier will first obtain Juniper's consent, either on its own behalf or on behalf of the relevant Data Subject.
4. If Juniper provides to Supplier pseudonymized Personal Data such that the data cannot be identified to a Data Subject without use of additional information that is held only by Juniper, Supplier shall not attempt to reidentify the pseudonymized Personal Data, and any Government Request for pseudonymized Personal Data should be handled in accordance with Section 8 in the DPA.