Reseller Data Protection and Privacy Exhibit

This Reseller Data Protection and Privacy Exhibit (the "**DPA**") is entered into by and between Juniper Networks, Inc. on behalf of itself and any of its Affiliates ("**Juniper Networks**") to whom the Reseller provides resale Services and the reseller ("**Reseller**") named in a Master Purchase and License Agreement with Channel Schedule or Special Terms or other contract ("**Main Agreement**") under which Reseller has been engaged to resell ("**Resale Services**") Juniper products and/or services ("**Juniper Products and Services**") to end user customers ("**Customers**"). Juniper and Reseller are each a "**Party**" and collectively the "**Parties**."

1. Definitions. Terms used in this DPA shall have the meaning indicated below unless otherwise defined in this DPA.

1.1. "**Affiliate**" means a company controlling, controlled by, or under common control with a Party.

1.2. "**Business Contact Data**" shall mean Personal Data of any Juniper or Reseller employees, contractors, customers, or partners that is Processed by a Party on behalf of the other.

1.3. "**Data Protection Requirements**" shall mean any laws, regulations, statutes, directives, orders, and rules related to the Processing of Personal Data by a Party.

1.4. "**Personal Data**," "**Data Subject**," "**Supervisory Authority**," "**Process**," "**Processor**," and "**Controller**," "**Sell**," "**Share**," and "**Service Provider**" will each have the meaning given to them (or their similar terms) in applicable Data Protection Requirements.

1.5. "**Support Data**" shall mean any Personal Data processed for purposes of technical support that are provided by Reseller to Juniper Networks in connection with the Main Agreement.

1.6. "**Standard Contractual Clauses**" means: (i) the Standard Contractual Clauses annexed to 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 4.4 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**").

Any other terms that are capitalized but not defined below, shall have the meanings set forth as defined in Data Protection Requirements and/ or the Main Agreement, as applicable.

2. General Provisions.

2.1. Processing Roles. For both Business Contact Data and Support Data, the Party providing the data shall be the "**Discloser**" and the party receiving the data shall be the "**Recipient**." As between the Parties and if applicable under Data Protection Requirements:

2.1.1. Discloser and Recipient are each a Controller of Business Contact Data exchanged under the Main Agreement.

2.1.2. Reseller and Juniper Networks are each a Processor, Subprocessor, or "Service Provider," as applicable, of Support Data depending on Reseller's relationship with the Customer.

2.2. Additional Processing Terms. Recipient will only Process Support Data on behalf of Discloser and in accordance with Recipient's written instructions as set forth in the Main Agreement and this DPA. If Recipient determines that additional Processing of Support Data is required by Data Protection Requirements, it shall inform Discloser of the applicable requirement in writing before such Processing (to the extent permitted by applicable law). Any additional or different instructions require a signed agreement between the Parties and may be subject to additional fees. For the avoidance of doubt, Discloser's instructions for the Processing of Support Data shall comply with Data Protection Requirements. Discloser shall have sole responsibility for the accuracy, quality, and legality of Support Data and the means by which Discloser acquired Support Data. Recipient will immediately inform Discloser if, in its opinion, an instruction from Discloser infringes the Data Protection Requirements, provided, however, Recipient is not responsible for performing legal research and/or for providing legal advice to Discloser. No Personal Data is Processed under the DPA as consideration for any Resale Services or

Juniper Products and Services. Recipient will not Process Business Contact Data for any purposes incompatible with the intended purpose of the disclosure to Recipient.

2.3. If Recipient cannot Process Support Data according to Discloser's instructions due to a legal requirement under any Data Protection Requirements, Recipient will promptly notify Discloser of such inability, 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.

2.4. Support Data transmitted by Reseller to Juniper Networks may not include any sensitive or special data that imposes specific data security or data protection obligations on Recipient in addition to that which is necessary for Juniper Networks to address a support case, or which are not provided as part of the Juniper Products and Services or Resale Services.

2.5. Subject matter and other details of Recipient's Processing of Personal Data are set forth in Schedule 1. Recipient shall Process Personal Data for an indefinite term for as long as the Main Agreement is in effect and thereafter as permitted by Data Protection Requirements or other applicable laws.

2.6. If and to the extent there are conflicts between this DPA (excluding its Schedules) and the Schedules, the applicable Schedule(s) shall prevail, unless otherwise required under Data Protection Requirements.

3. Additional US Privacy Obligations. To the extent required under applicable US Data Protection Requirements, Recipient: (i) shall not Sell or Share Support Data or Business Contact Data; (ii) shall retain, use, or disclose Support Data or Business Contact Data only to provide the Products and Services or Resale Services, as applicable, and shall not retain, use, or disclose Support Data or Business Contact Data for any other purpose, except as may be permitted by applicable US Data Protection Requirements or this Agreement; (iii) shall not retain, use, or disclose Support Data or Business Contact Data collected by Discloser outside of the direct business relationship between the parties, except as may be permitted by applicable US Data Protection Requirements or this Agreement; (iv) grants Discloser the right, upon notice, and consistent with the terms in Section 16, to take reasonable and appropriate steps to stop and remediate Recipient's unauthorized use of Support Data or Business Contact Data as permitted by applicable US Data Protection Requirements; (vi) shall not combine Business Contact Data with Personal Data that Recipient receives from or on behalf of another person(s), except as permitted by applicable US Data Protection Requirements; and (v) shall notify Discloser if it determines that it can no longer meet its obligations under US Data Protection Requirements. Recipient certifies that it understands and shall comply with the restrictions under Sections 3(i), 3(ii), 3(iii), and 3(iv) of this Agreement.

4. International Transfers.

4.1. Recipient may Process Personal Data on a global basis as necessary to provide the Juniper Products and Services or Resale Services, as applicable, including for IT security purposes, maintenance and provision of the Juniper Products and Services and related infrastructure, technical support, and change management. Without limiting Sections 4.2 through 4.6, Each Party shall implement technical and organizational measures consistent with this DPA to provide a comparable level of protection for Personal Data in the jurisdiction in which it is Processed. Each Party shall comply with Schedule 2 in its Processing of Personal Data outside of the country from which the Personal Data originated.

4.2. To the extent that Recipient's Processing of Personal Data involves the transfer of such Personal Data from the European Economic Area ("**EEA**") to a country or territory outside the EEA, other than a country or territory that has received a binding adequacy decision as determined by the European Commission (an "**EEA Transfer**"), such EEA Transfer shall be subject to the EU SCCs as set forth below.

4.3. Discloser shall be deemed to have signed the EU SCCs in its capacity of "data exporter" and Recipient in its capacity as "data importer." Modules One, Two, or Three of the EU SCCs shall apply to the transfer depending on the roles of the Parties in accordance with Section 2.1. If Module Three applies, Reseller notifies Juniper Networks that Reseller is a Processor and the instructions shall be as set forth in Section 2.2. With regards to optional clauses within the EU SCCs, Clause 7 is not selected and the optional paragraph within Clause 11 is not selected. For purposes of Clauses 17 and 18 of the EU SCCs, the Parties select The Netherlands.

4.4. Where Personal Data originating from the United Kingdom specifically is processed by Recipient outside of the United Kingdom, in a territory 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 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 Personal Data, subject to the UK Addendum, which is completed as follows: (i) Table 1, 2, and 3 of the UK Addendum completed with the information within Schedule 1, attached hereto, and in accordance with the information set forth within Sections 4.3 and 9; and (ii) and the option "neither party" is selected in Table 4.

4.5. 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.

4.6. In the event of any conflict between any terms in the Standard Contractual Clauses and this DPA, the Standard Contractual Clauses shall prevail to the extent of the conflict. The Standard Contractual Clauses will cease to apply if Recipient implements an alternative recognized compliance mechanism for the lawful transfer of Personal Data in accordance with Data Protection Requirements, in which case such alternative mechanism shall apply.

5. Bundling of Entities. The Parties agree that the bundling of a Party's entities, for example, if a Party is comprised of multiple global affiliates, as Controllers or Processors within this single DPA is undertaken for efficiency purposes (*i.e.*, to avoid a multitude of different contract documents) and (i) shall result in legally separate DPAs between the respective entities solely for purposes of addressing any such obligations under Data Protection Requirements; (ii) shall not create any new or different legal or other relationship whatsoever between the "bundled" entities of each Party; (iii) does not create any additional rights or remedies for such bundled entities of each Party; (iv) all Processing instructions must be provided by the Discloser entity that is signatory to the Main Agreement and Recipient is not responsible for consolidating or evaluating the validity of instructions received from bundled Discloser entities; (v) any commercial terms not provided by the DPA are provided by the Main Agreement regardless of whether the bundled Discloser entities signed or were consulted regarding the terms of the Main Agreement; and (vi) any audits conducted in accordance with the DPA shall be conducted by and through the Discloser entity that is signatory to the Main Agreement.

6. Data Protection Compliance. Each party undertakes to comply with the Data Protection Requirements applicable to such party's Processing of Personal Data in connection with the Main Agreement. Prior to disclosing Business Contact Data to Recipient, Discloser, if a Controller, shall provide all required notices, obtain all permissions or, if applicable and sufficient under Data Protection Requirements, apply another valid legal basis required under Data Protection Requirements.

7. Data Secrecy and Confidentiality. Unless permitted by the Data Protection Requirements, Recipient shall treat the Personal Data Processed as confidential and shall not disclose such data to any third parties unless authorized by the Discloser and in accordance with this DPA. This obligation continues to apply after the expiration or termination of this DPA for so long as Recipient Processes Personal Data. In accordance with Data Protection Requirements, Recipient shall put procedures in place designed to ensure that all persons acting under its authority entrusted with the Processing of Personal Data (i) have committed themselves to keep such data confidential and not to use such data for any purposes except for the provision of the Juniper Products and Services or Resale Services, as applicable, or (ii) are under an appropriate statutory obligation of confidentiality. This obligation to confidentiality shall continue after the end of the respective engagement of such person. Recipient will further instruct such persons regarding the applicable statutory provisions on data protection and shall ensure that access to Personal Data is limited to those persons with a need to know.

8. Security Measures. 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, Recipient will implement appropriate technical and organizational measures designed to protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data (described in Annex II within Schedule 1). Recipient may update its security practices from time to time but will not materially decrease the overall protection of such security measures during the term of the Main Agreement. Such measures shall include process for regular testing, assessing and evaluating the effectiveness of the measures.

9. Subcontracting Authorization. When subcontracting the Juniper Products and Services or Resale Services or parts thereof, as applicable, to another entity or a third party, if the subcontractor will Process Personal Data, such subcontractor shall be a Subprocessor and the Recipient engaging such Subprocessor will enter into a binding written agreement with the Subprocessor that imposes on the Subprocessor the same level of restrictions that apply to Recipient under this DPA as well as any terms required to be included under applicable US Data Protection Requirements, in each case to the extent that such requirements are

applicable to the Processing to be done under such subcontract. Recipient shall provide Discloser a list of its Subprocessors upon request or provide a link to a published list of Subprocessors. For the avoidance of doubt and in accordance with Clause 9, Option 2 of the Standard Contractual Clauses for Modules Two and Three, the above constitutes Discloser's general authorization for Recipient's engagement of Subprocessors and its appointment of additional Subprocessors or replacement of any Subprocessors. Discloser agrees to provide any objections to Subprocessors promptly, provided such objections are based on documented evidence that establish the Subprocessor does not or cannot comply with this DPA or Data Protection Requirements and identify the reasonable data protection basis for the objection ("**Objection**"), so that Recipient can evaluate the Objection and determine any appropriate action. In the event of an Objection, Discloser and Recipient will work together in good faith to find a mutually acceptable resolution to address such Objection, including but not limited to reviewing additional documentation supporting the Subprocessor's compliance with the DPA or Data Protection Requirements.

10. Personal Data Breach Notification.

10.1. Recipient will provide Discloser promptly with a data breach notification (with contents detailed below) if Recipient becomes aware of and confirms any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data or any other security incident that compromises the security, confidentiality or integrity of Personal Data that requires a data breach notification to Discloser according to Data Protection Requirements (**"Personal Data Breach"**). Discloser and Recipient shall work together in good faith within the timeframes for Discloser to provide notifications in accordance with Data Protection Requirements to finalize the content of any such notifications to Data Subjects or Supervisory Authorities, as required by Data Protection Requirements. Recipient's prior written approval shall be required for any statements regarding, or references to, the Personal Data Breach or Recipient made by Discloser in any such notifications.

10.2. As information regarding the Personal Data Breach becomes available for Recipient to disclose to Discloser, Recipient will provide Discloser with information regarding the Personal Data Breach as required by Data Protection Requirements and, upon written request, other information concerning the Personal Data Breach reasonably known or available to Recipient. Juniper Networks' contact point for additional details regarding a Personal Data Breach is privacy@juniper.net and Reseller's is the primary contact person identified by Reseller to Juniper Networks in the Juniper partner portal.

11. Support Data Recipient Handling of Complaints, Inquiries and Orders. Recipient shall notify Discloser of a Data Subject's complaint or inquiry (e.g., regarding the rectification, deletion and blocking of or the access to Personal Data, or any other rights Data Subject has under Data Protection Requirements) (**"Data Subject Inquiry"**) received by Recipient relating to the Juniper Products and Services or Resale Services, as applicable, covered by the Main Agreement. Recipient shall not independently respond to Data Subject Inquiries without Discloser's prior approval, except where required by Data Protection Requirements. The same shall apply to orders and inquires of courts or regulators. To the extent Discloser does not have the ability to address a Data Subject Inquiry, Recipient shall provide reasonable assistance to Discloser to respond to such Data Subject Inquiry in a timely manner. Recipient shall assist Discloser by appropriate technical and organizational measures, insofar as this is possible, in the fulfilment of Discloser's obligations to respond to Data Subject Inquiries under Data Protection Requirements. Recipient will instruct Data Subjects that do not identify a relevant Controller to contact the correct Controller. Recipient shall comply with Discloser's instructions regarding the handling of a Data Subject Inquiry, subject to the terms of Section 2.2.

12. Term. The term of this DPA is identical with the term of the Main Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the Main Agreement.

13. Data Retention. After the end of the provision of the Juniper Products and Services or Resale Services, as applicable, and pursuant to written instructions provided by Discloser, Recipient shall return to Discloser or securely destroy all copies of Support Data Processed on behalf of Discloser in Recipient's role as a Processor (or Subprocessor). Recipient may retain Support Data to the extent required by applicable laws only for such period as required by applicable laws, or as necessary to protect its legal rights, and provided that Recipient shall protect the confidentiality of all such Support Data and Process such Support Data only as necessary for the relevant purpose(s) requiring its storage and for no other purpose. Each party shall retain its Business Contact Data for which it is a Controller in accordance with its data retention policies and Data Protection Requirements.

14. Invalidity and/or Unenforceability. Should any provision of this DPA be found invalid or unenforceable by a competent court of law, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, should this not be possible, construed in a manner as if the invalid or unenforceable part had never been contained therein.

15. **Liability.** Indemnification, liability, limitations of liability and any applicable exclusions under this DPA shall be governed by the Main Agreement to the extent permitted by Data Protection Requirements.

16. **Corporate Restructuring**. Recipient may share and disclose Personal Data and other data of Discloser in connection with, or during the negotiation of, any merger, sale of company assets, consolidation or restructuring, financing, or acquisition of all or a portion of Recipient's business by or to another company, including the transfer of contact information and data of customers, partners and end users.

17. **Information, Audits, and Assistance.**

17.1. Upon Discloser's written request, and subject to the confidentiality obligations set forth in the Agreement, Recipient shall make available to Discloser information reasonably necessary to substantiate Recipient's compliance with this DPA as to Recipient's Processing of Support Data and to assist Discloser with complying with its obligations under Data Protection Requirements. Upon request and if available for the Products and Services in scope, Recipient will provide evidence of its compliance with established security protocols (such as ISO27001 or SOC2 Type 2). If none of the information set forth in this paragraph is available at the time of Discloser's request, Recipient will allow and cooperate in audits as set forth below.

17.2. Discloser shall have the right to carry out remote audits via videoconferencing services (e.g. Microsoft Teams, Zoom). Discloser shall have the right to carry out on-site audits (no more than once per year), during regular business hours without disrupting the Recipient's business operations regarding its Processing of Support Data and in accordance with the Recipient's security policies. Any third party engaged by Discloser to conduct an audit must be pre-approved by Recipient (such approval not to be unreasonably withheld) and sign Recipient's confidentiality agreement. Discloser may carry out audits in accordance with this section on site if Discloser has a right to do so under Data Protection Requirements.

17.3. For any audits, Discloser must provide Recipient with a proposed audit plan at least two weeks in advance of the audit, after which Discloser and Recipient shall discuss in good faith and finalize the audit plan prior to commencement of audit activities. Each party shall bear responsibility for any costs or expenses it incurs in connection with an audit. Information obtained or results produced in connection with an audit are Recipient's confidential information and may only be used by Discloser to confirm Recipient's compliance with this DPA and to comply with Discloser's obligations under Data Protection Requirements.

17.4. If requested by Discloser solely in order to support Discloser's compliance with Data Protection Requirements as to Recipient's Processing of Support Data, Recipient shall provide, at Discloser's expense, reasonably required assistance to Discloser in ensuring its compliance relating to data protection impact assessments and prior consultation with Supervisory Authorities, taking into account the nature of the processing and the information available to Recipient. All such information provided shall be Recipient's confidential information.

18. **Amendments for Additional Local Data Protection Requirements.** To the extent that additional country-specific (or state, or regional, provincial, or other geographic area specific) provisions are required under Data Protection Requirements, the Parties agree to incorporate such provisions solely to the extent they are required and solely to the extent they are applicable to particular Personal Data processed by Recipient. Juniper Networks may, from time to time, post updated provisions related to local or other specific Data Protection Requirements on the Juniper Privacy Policy available at https://www.juniper.net/us/en/privacy-policy under the heading Additional Local Provisions. Such posted provisions are automatically incorporated herein solely to the extent they are required under Data Protection Requirements.

SCHEDULE 1

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES

ANNEX I

A. LIST OF PARTIES

Data Exporter:
Name: The Data Exporter is the entity identified "Discloser" in the DPA.
Address: as set forth in the Main Agreement.
Contact person: as set forth in the Notices provision in the Main Agreement.
Activities relevant to the data transferred under these Clauses: as set forth in the Main Agreement.
Signature and date: refer to DPA.
Role: Controller of Business Contact Data and Processor or Subprocessor of Support Data.

Data Importer:
Name: The Data Importer is the entity identified as "Recipient" in the DPA.
Address: as set forth in the Main Agreement.
Contact person: as set forth in the Notices provision in the Main Agreement.
Activities relevant to the data transferred under these Clauses: as set forth in the Main Agreement.
Signature and date: refer to DPA.
Role: Controller of Business Contact Data and Processor or Subprocessor of Support Data.

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects: The Personal Data transferred concern the following categories of data subjects:

- Data Exporter Personnel (including employees, contractors, interns, and other temporary workers)
- Data Exporter Customers (including their employees, contractors, interns, other temporary workers, and other users)
- Data Exporter Business Partners (including partners, suppliers, and other vendors)

Categories of Personal Data transferred: The Personal Data transferred concern the following categories of data in addition to any other categories as specified in: (a) the Main Agreement; (b) the Juniper Networks Privacy Policy available at https://www.juniper.net/us/en/privacy-policy/ together with any Supplemental Privacy Information referenced therein (including for Mist Systems) or Reseller's Privacy Policy (collectively, "**Privacy Policies**"); and (c) in any data sheets or related product documentation provided by Juniper Networks for the particular Juniper Product and Services ("**Documentation**"):

- Business Contact Data (as defined in the DPA).
- Support Data (as defined in the DPA):
    - Network Devices: Occasionally, Customer or its end users' IP addresses, and less frequently, core dump files or network traffic snippets from a network device, may also be provided when requesting support and could be deemed to contain Personal Data to the extent it can be associated with an individual data subject.
    - Cloud Services: For Juniper Products and Services that include Cloud services, the categories of data that may be processed are as set forth in the Juniper Networks Privacy Policy and Documentation.
    - WLAN: For WLAN products and services of Juniper Networks, such as from its affiliate Mist Systems, Inc., the categories of data that may be processed are as set forth in the Juniper Networks Privacy Policy and Documentation.
    - Professional Services: Any Personal Data that is shared with Juniper Networks by or on behalf of Reseller in connection with any professional services provided by Juniper Networks under the Main Agreement.

Supplemental product-specific information: Additional information regarding data processing related to particular Juniper Products and Services is available in the "**Supplemental Privacy Information**" section of the Juniper Networks Privacy Policy.

Sensitive categories of data (if appropriate): The Personal Data transferred concern the following special categories of data:
Data Importer does not require any special categories of data. Unless otherwise specified in the Main Agreement, Data Exporter shall not provide and must receive prior written consent of Data Importer before transferring any special categories of data or sensitive data to Data Importer.

The frequency of the transfer: As set forth in the Main Agreement.

Nature of the Processing: The Personal Data transferred will be subject to the following basic processing activities:

> Providing the Juniper Products and Services and Resale Services in connection with the Main Agreement, providing related technical support and professional services under the Main Agreement (as applicable), and improving/enhancing such Juniper Products and Services, Resale Services, and related support services.

Data Importer also retains the right to process the Personal Data for purposes including enforcing its legal rights, complying with legal requirements, providing information on Juniper Products and Services, training resources, and opportunities for upgrades and enhancements, and other permitted purposes under applicable law, as set forth in the Privacy Policies.

Purposes of the data transfer and further Processing: The processing activities defined in Section 2 of the DPA and in the Main Agreement.

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period: As set forth in the DPA and Main Agreement.

For transfers to (sub-) Processors, also specify subject matter, nature and duration of the Processing: As set forth in the DPA and the Main Agreement.

C. COMPETENT SUPERVISORY AUTHORITY
If the Data Exporter is established in an EU Member State, the competent Supervisory Authority shall be the Supervisory Authority applicable to the establishment location of the Data Exporter. If the Data Exporter is not established in an EU Member State, the competent Supervisory Authority shall be the Supervisory Authority located where the Data Exporter has appointed its EU Representative. If the Data Exporter is not established in an EU Member State and is not required to appoint an EU Representative, the competent Supervisory Authority shall be the supervisory authority applicable to the location of the Data Subject whose data is at issue.

ANNEX II

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

1. **Information Security Governance**
   - The information security function within Data Importer reports directly to a company executive.
   - A Security and Privacy Steering Committee made up of representatives from business, information security, and privacy meets regularly to discuss and review information security policies, projects, and practices.
   - A comprehensive set of information security policies and standards are documented, approved, and regularly reviewed.
   - Personnel with access to Personal Data are subject to confidentiality obligations.

2. **Network Security**
   - Network security is maintained using industry standard techniques, including, for example, firewalls, intrusion detection systems, access control lists, and routing protocols.
   - Network, application, and server authentication passwords are required to meet minimum complexity guidelines (at least 12 characters with at least three of the following four classes: upper case, lower case, numeral, special character) and be changed periodically.
   - WiFi networks are secured and encrypt data in transit. Guests are permitted to connect only to the guest WiFi network and are not allowed to connect to any production systems.
   - An intrusion detection or prevention system covers network traffic to the Data Importer information systems.
   - Network changes are tested prior to production deployment.
   - Firewalls are appropriately configured and implemented. Firewall policies are reviewed on a regular basis.
   - Employees and contractors are required to use VPN to connect remotely to the corporate network.

3. **Encryption**
   - Full disk encryption is configured on Data Importer-managed end point devices.
   - Encryption methods for Data Importer's systems which Process Data Exporter Personal Data are based on factors such as length of time such data are Processed, technical capabilities of third-party attackers, Data Importer's resources, and sensitivity of the Personal Data.
   - Encryption keys to Data Exporter's Personal Data are stored in a key management solution. Keys are rotated periodically and access to keys is restricted to limited personnel with administrative access only. Membership for encryption key ownership groups is regularly reviewed according to a written Encryption Key Management Standard.
   - Sensitive Personal Data is encrypted in transit and at rest in compliance with Data Importer's Information Security Cryptographic Policy.

4. **Identity and Access Management**
   - Data processing systems handling Personal Data are subject to measures designed to prevent access, loss or use without authorization.
   - Employees or contractors with access to Personal Data are assigned unique IDs.
   - Only authorized staff may grant, modify, or revoke access to Data Exporter's Personal Data. The list of authorized staff is regularly reviewed.
   - Systems processing personal data are required to integrate with Data Importer's single sign on authentication.
   - Access rights are assigned using the principle of least privilege and need-to-know.
   - Access is revoked upon termination of the employee or contractor.
   - Login attempts are limited and accounts locked after a predetermined number of failed login attempts.
   - Remote access for critical applications is controlled via multi-factor authentication.
   - Systems processing Data Exporter's Personal Data implement session or screen lockouts after a predetermined period of inactivity.

5. **Physical Security**
   - Physical access to Data Importer buildings by unauthorized personnel is restricted.
   - Physical access controls, such as surveillance cameras and identification badges, are implemented for Data Importer's facilities.

- Physical security systems such as fire suppression systems, flood controls, smoke detection, and UPS are utilized.
- Data Importer has implemented significant physical security measures such as perimeter security, access control, CCTV and alarm monitoring, visitor screening and control, security guarding and reception services, and 24-hour Security Operations Centers for monitoring and incident response.

6. Patch and Vulnerability Management

- Anti-malware and anti-virus software are in place and are updated on a regular cadence, including for Data Importer's managed devices handling Personal Data.
- Data Importer implements a patch management program designed to ensure security patches are appropriately applied to systems.
- Vulnerability scans for systems processing Data Exporter's Personal Data are performed on a periodic basis.
- Any known critical vulnerabilities as defined by Data Importer's risk assessment are assessed and remediated in a timely manner.

  Annual penetration tests are conducted for certain Data Exporter-facing systems.

7. Continuous System Monitoring

- Audit logging is implemented in production system. Audit logs are retained for appropriate periods, including as required by applicable regulatory requirements.
- Data Importer reviews and analyses information system audit records for indications of unusual activities.

8. Business Continuity Management

- Emergency and contingency plans are available and maintained in an effort to restore Personal Data, where applicable, as reasonably deemed appropriate by Data Importer.
- Business continuity plans are tested and updated on a periodic basis, as reasonably deemed appropriate by Data Importer.
- Backups of data are maintained for business continuity purposes, as reasonably deemed appropriate by Data Importer.

9. Incident Response

- Data Importer maintains a written Incident Response plan providing a standard process to investigate and address security incidents and regularly reviews the Incident Response plan.
- Data Importer will notify Data Exporter of Personal Data Breaches in accordance with the DPA and its Breach Notification Plan.
- Data Exporter may contact Data Importer as set forth in the DPA for any available details regarding a Personal Data Breach.

10. Security Awareness

- Background checks are required on personnel at the time of hire, to the extent permitted under applicable law.
- Employees are required to undergo periodic privacy and information security training.
- Training is updated as deemed necessary by Data Importer.

11. Third Party Risk Management

- Sub-processors undergo a vendor information security review as appropriate based on their Personal Data access and are required to comply with vendor security requirements.
- Data Importer has a program to review the information security risk and control of third-party service providers. The review is performed on new and existing vendors. This includes reviews of the effectiveness of the controls of our third-party service providers who process Personal Data, for example through review of their SOC-2 Reports.

12. Secure Development

- Data Importer maintains a secure development program that includes measures such as secure coding practices; use of industry-standard practices to mitigate and protect against vulnerabilities; separate coding environments; source code vulnerability scanning; pre-release source code and application testing; and review of any open source of third-party code prior to its use.

13. Additional and/or Supplemental Technical Security Measures

- Additional and/or supplemental technical security measures, and appropriate modifications to the measures listed above, may be established by Data Importer periodically depending on the Juniper Products and Services, or Resale Services, offered and the type of Personal Data of Data Exporter that is Processed by Data Importer.
- Data Importer's policy does not permit BYOD or personally-owned devices to process Support Data.
- In assisting Data Exporter with fulfilling data subject requests, Data Importer shall either (a) provide to Data Exporter an online self-service solution to enable Data Exporter to fulfill data subject requests or (b) otherwise provide reasonable means for Data Exporter to submit requests.
- A change control process is in place for changes to Data Importer production systems.
- Personal Data hosted for different Data Importer customers are logically separated.
- Storage media for customer-facing systems are either destroyed or securely erased at the end of their lifecycle.
- Data Importer incorporates privacy by design and privacy by default practices in its solution development processes.

ANNEX III

List of Data Importer's Subprocessors

For Juniper Networks, please refer to Section 9 in the DPA.

SCHEDULE 2

The following provisions are based on European Data Protection Board Recommendations 01/2020 but will apply to the Processing of Personal Data outside of the country from which the Personal Data originated.

1. Recipient shall unless otherwise prohibited by law or a legally binding order of an applicable body or agency promptly notify Discloser of any request for the disclosure of Discloser Personal Data by a governmental or regulatory body or law enforcement authority (including any Supervisory Authority) ("**Disclosure Request**") without responding to such request, unless otherwise required by applicable law (including to provide acknowledgement of receipt of the request). Recipient will review applicable law to evaluate any Disclosure Request, for example the ability of the requesting authority to make the Disclosure Request, and to challenge the Disclosure Request if, after a careful assessment, it concludes that there are grounds under applicable law to do so. When challenging a Disclosure Request, Recipient shall seek interim measures to suspend the effects of the Disclosure Request until an applicable court or other authority has decided on the merits. Recipient shall not disclose Discloser Personal Data requested until required to do so under applicable law. Recipient shall only provide the minimum amount of Discloser Personal Data permissible when responding to the Disclosure Request, based on a reasonable interpretation of the Disclosure Request. If the Disclosure Request is incompatible with the Standard Contractual Clauses or other data transfer mechanism utilized in accordance with Section 4 in this DPA, Recipient will so notify the requesting authority and, if permitted by applicable law, notify the competent EEA government authority with jurisdiction over the Discloser Personal Data subject to the Disclosure Request. Recipient will maintain a record of Disclosure Requests and its evaluation, response, and handling of the requests. Recipient will provide Discloser with such records relevant to Discloser Personal Data except as prohibited by applicable law or legal process or in the interest in protecting Recipient's legal rights in connection with threatened, pending, or current litigation.
2. Recipient has not purposefully created "back doors" or similar programming in its systems that Process Discloser Personal Data that could be used to access the systems and/or Discloser Personal Data, nor has Recipient purposefully created or changed its business processes in a manner that facilitates access to Discloser Personal Data or its systems that Process Discloser Personal Data. To the best of Recipient's knowledge, United States Data Protection Requirements do not require Recipient to create or maintain "back doors" or to facilitate access to Discloser Personal Data or systems that Process Discloser Personal Data or for Recipient to possess or provide the encryption key in connection with a United States Disclosure Request.
3. Recipient shall use reasonable efforts to assist Discloser and its Data Subjects, as instructed by Discloser (in accordance with Section 11 of the DPA), regarding Disclosure Requests, unless prohibited by applicable law, for example to provide information to Discloser in connection with the Data Subject's efforts to exercise its rights and obtain legally-available redress, provided Recipient shall not be required to provide Discloser or Data Subjects with legal advice.
4. Discloser may request to audit Recipient information regarding access to Discloser Personal Data, subject to the terms of Section 16 of the DPA.
5. Recipient has established an internal procedure regarding handling of Disclosure Requests and applicable transfers of Discloser Personal Data. Recipient has procedures for applicable personnel to receive information, as appropriate, regarding applicable transfers of Discloser Personal Data, where such information may include an explanation of the necessity of the transfer and any data protection safeguards in scope.
6. In the event Recipient receives a request to voluntarily disclose unencrypted Discloser Personal Data to a government authority, Recipient will use reasonable efforts to first obtain Discloser's consent, either on its behalf or on behalf of the relevant Data Subject.