JUNIPER VENDOR SECURITY REQUIREMENTS

INTRODUCTION

This document describes the measures and processes that the Vendor shall, at a minimum, implement and maintain in order to protect Juniper Data against risks inherent in the Processing and all unlawful forms of Processing, including but not limited to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Juniper Data transmitted, stored or otherwise processed. Vendor shall keep any necessary written records and documentation (including in electronic form) to 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 specific statutory requirements for technical and organizational measures that may be applicable.

1. DEFINITIONS

a) Contract: The master services agreement or other contract between the parties under which the Vendor provides Products and/or Services to Juniper.
b) Incident or Security Incident: Any event or set of events that indicates an attack upon, unauthorized use of, or attempt to compromise computing or networking systems that may lead to a Data Breach.
c) Internal Systems: Devices that perform computing or networking services to provide or support Vendor's Services.
d) 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.
e) Juniper: Juniper Networks, Inc. and its affiliates, where "affiliates" are entities controlling, controlled by, or under common control with Juniper Networks, Inc.
f) Juniper Data: any proprietary or 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 Vendor or the Products and Services.
g) Juniper Systems: devices and information technology resources owned, operated, or otherwise made available to Vendor by Juniper that transmit, process, handle, store, modify, or make available for access Juniper Data.
h) Data Breach: Any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Juniper Data transmitted, stored or otherwise processed.
i) 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. Vendor 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 Vendor, to the Vendor'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. Vendor implements the following controls to maintain the security and integrity of Information Systems utilized in Processing Juniper Data.

i. Vendor shall use industry security resources (e.g., National Vulnerability Database "NVD", CERT/CC Advisories, CISA's KEV Catalog) to monitor for security alerts.

ii. Vendor 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. Vendor implements and maintains network security measures including the following:
   i. Vendor'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.
   vii. 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 Vendor 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 Vendor's premises or network, Vendor 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. Vendor 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 Vendor accesses Juniper Systems, whether to process Juniper Data or for any other reason,

Vendor shall comply with Juniper's then-current Information Security requirements.

iv. In the event Vendor processes Juniper Data using its Information Systems, Internal Systems, or other Vendor resources, Vendor shall implement and maintain the controls and practices set forth in this Exhibit.

v. Vendor'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 Vendor 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) Vendor must have documented and implemented backup procedures.
   (2) Vendor must have a documented disaster recovery plan that is tested at least annually.

vii. Retention, Erasure, Destruction and Return
   (1) Vendor 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 Vendor 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

Vendor 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. Vendor shall not change its business processes that would facilitate access to Internal Systems, Juniper Systems, or Juniper Data. Vendor represents and warrants that no laws or government policies applicable to Vendor 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 Vendor's software or hardware does not undermine the security posture of the Vendor or Juniper.

8. AUDITS OR ASSESSMENTS

a) Vendor 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 Vendor'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.

Vendor:_____

Signature: _____

Name: _____

Title: _____

Date: _____