Juniper Vendor Security Requirements

INTRODUCTION

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

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

DEFINITIONS

1. Information Systems: Information technology resources that transmit, process, handle, store, modify, or make available for access, Juniper information and provide services as a part of this agreement.
2. 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.
3. Data Breach: Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Juniper Data transmitted, stored or otherwise processed.

2. SYSTEM SECURITY

a. Access controls.
   i. Unique IDs must be assigned to all individual users.
   ii. Procedures for timely access removal must be implemented and regularly assessed.
   iii. The principles of least privilege and need to know must be implemented and followed.
   iv. The principles of least privilege and need to know must be regularly reviewed on a periodic basis (e.g. regular account and access reviews).
   v. Passwords:
      (1) Passwords must be a minimum of 8 characters in length.
      (2) Password complexity must contain at least three of the following four criteria: (i) one uppercase letter, (ii) one lowercase letter, (iii) one number, and (iv) one special character.
      (3) Passwords must be changed at least once every ninety (90) days.
      (4) Passwords cannot be any of the five (5) previous passwords.
      (5) Initial or temporary passwords must be changed after first use.
      (6) Default passwords must be changed upon deployment.
      (7) Passwords must never be sent in clear text format.
      (8) Passwords must not be shared amongst users.
   vi. Authentication:
      (1) Authentication credentials must be protected by encryption during transmission.
      (2) Login attempts must be limited to no more than five (5) consecutive failed attempts with the account being locked out for at least five (5) minutes upon reaching

the limit.

(3) Remote administration access, by the Vendor, to the Vendor's Information Systems that can access Juniper data shall use two (2) factor authentication.

vii. Sessions:

(1) A password-protected screensaver must be activated when user sessions are inactive for fifteen (15) minutes.

(2) Management systems, such as jump stations or bastion hosts, must time out sessions at regular intervals not to exceed twelve (12) hours.

b. Scanning and administration.

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

3. NETWORK SECURITY

a) Network.

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

4. END USER DEVICES

a) Laptops and desktops.

i. Full-disk encryption must be implemented.

b) Smartphones and tablets.

i. Smartphones and tablets must not be allowed to access, process, or store Juniper data.

c) Bring Your Own Device (BYOD).

i. If allowed on Vendor's premise 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. An Information Security Policy must be implemented and reviewed on an at least an annual basis.
ii. The Information Security Policy must be approved by the CISO, CIO, or appropriate executive.
iii. All employees, contractors, and subcontractors with access to Juniper data must agree to comply with the Information Security Policy.
iv. Subcontractors must comply with the requirements outlined in this document.

b) Data protection requirements.

i. Transport
   (1) Encrypt the transfer of Juniper data, including backups, over external networks.
   (2) Encrypt Juniper data when transferred via physical media.
ii. Storage
   (1) Encrypt Juniper data, including backups, at rest.
iii. Business Continuity
   (1) A documented business continuity plan must be implemented.
iv. Backup and Recovery
   (1) Documented backup procedures must be implemented.
   (2) A documented and tested disaster recovery plan must be implemented.
v. Retention, Erasure, Destruction and Return
   (1) A documented policy for retention, secure erasure, destruction or return of Juniper data must be implemented.
   (2) Information assets containing Juniper data must be either destroyed or securely erased at the end of their lifecycle.
vi. Separation of processing for different purposes
   (1) Where necessary to ensure Juniper data is only available to authorized persons, implement measures to make sure that data collected for different purposes can be processed separately.
vii. Customer separation
   (1) Juniper data must be logically or physically separated from the data of other customers.
viii. Classification
   (1) A classification policy and handling practices must be documented to protect Juniper data.
ix. Third parties
   (1) Third parties may only be granted access to Juniper data upon Juniper Networks' permission for each single case or as permitted under the services agreement signed between Juniper Networks and the Vendor (e.g., as regards commissioning of subcontractors).

6. INCIDENT RESPONSE

a) Plan and point of contact.

i. A documented incident response plan must be maintained.
ii. A helpline or e-mail contact must be provided for employees or contractors to report security incidents.

iii. Determine if an incident has resulted in a Data Breach or is reasonably suspected to have resulted in a Data Breach and take immediate actions to mitigate it.

b) Data Breach notification.

i. Notification to Juniper of a Data Breach must occur without undue delay and no later than twenty-four (24) hours after becoming aware of it.

ii. Data Breach notification must include:

(1) What happened and how many records are involved.

(2) The measures and mitigation steps taken or planned to be taken to address the Data Breach.

(3) The name and contact details for more information about the Data Breach.

7. SECURE DEVELOPMENT

a) Development requirements.

i. Develop, implement, and comply with industry-standard secure coding best practices.

ii. Follow industry-standard best practices to mitigate and protect against known and reasonably predictable security vulnerabilities, including but not limited to:

(1) unauthorized access

(2) unauthorized changes to system configurations or data

(3) disruption, degradation, or denial of service

(4) unauthorized escalation of user privilege

(5) service fraud

(6) improper disclosure of Juniper data

iii. Separate test and stage environments from the production environment.

iv. Non-production systems must not contain production data.

v. Scan source code for security vulnerabilities prior to release to production.

vi. Test applications for security vulnerabilities prior to release to production.

b) Open source and third party software.

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

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 Networks on request.

v. An annual penetration test must be performed by a third party.

9. TRAINING

a) Security and privacy training.

i. Information security and privacy training or awareness communications must be provided to all personnel with access to Juniper data upon hire and 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 16 or similar reports.

Further measures implemented by the Vendor:

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

[Vendor Name]

Signature: _____

Name: _____

Title: _____

Date: _____