

JUNIPER NETWORKS, INC.

NONDISCLOSURE AGREEMENT

THIS AGREEMENT is made on 29/03/2019 by and between JUNIPER NETWORKS, INC., a Delaware corporation, on behalf of itself and its affiliates and subsidiaries (together, the "Company"), and Ashutosh Tripathi ("Consultant"), an employee of Talentica Software (India) Pvt. Ltd. (insert ProUnlimited or other temp agency name as appropriate)

1. **Purpose.** The Company and Consultant have a consulting relationship under which each may disclose its Confidential Information to the other.

2. **Definition.** "Confidential Information" means any information, technical data, or know-how, including, but not limited to, that which relates to research, products, services, customers, markets, software, developments, inventions, processes, employee lists, designs, drawings, engineering, marketing or finances, which Confidential Information is designated in writing to be confidential or proprietary, or if given orally, is indicated orally at the time of disclosure as having been disclosed as confidential or proprietary. Notwithstanding the above, Confidential Information also includes any oral or written information which by its nature and the circumstances of its disclosure the receiving party should reasonably infer to be confidential or proprietary. Confidential Information does not include information, technical data or know-how which (i) is in the possession of the receiving party at the time of disclosure as shown by the receiving party's files and records immediately prior to the time of disclosure; or (ii) prior or after the time of disclosure becomes part of the public knowledge or literature, not as a result of any inaction or action of the receiving party, or (iii) is approved for release by the disclosing party.

3. **Non-Disclosure of Confidential Information by the Company.** The Company agrees not to disclose the Confidential Information of the Consultant to third parties or to the Company's employees except employees who are required to have the information in order to carry out the Company's business. The Company has had or will have employees to whom Confidential Information of the Consultant is disclosed sign the Company's standard non-disclosure agreement. The Company agrees that it will take all reasonable steps to protect the secrecy of and avoid disclosure or misuse of Confidential Information of the Consultant in order to prevent it from falling into the public domain or the possession of unauthorized persons. The Company agrees to notify the Consultant in writing of any misuse or misappropriation of such Confidential Information by the Company or its employees which may come to its attention.

4. **Non-Disclosure of Confidential Information by the Consultant**

a. Consultant will not, during or subsequent to the term of this Agreement, use the Company's Confidential Information for any purpose whatsoever other than the performance of Consultant's services on behalf of the Company or disclose the Company's Confidential Information to any third party, and it is understood that said Confidential Information shall remain the sole property of the Company. Consultant further agrees to take all reasonable precautions to prevent any unauthorized disclosure of such Confidential Information.

b. Consultant recognizes that the Company has received and in the future will receive from third parties their confidential or proprietary information subject to a duty on the



Company's part to maintain the confidentiality of such information and to use it only for certain limited purposes. Consultant agrees that Consultant owes the Company and such third parties, during the term of this Agreement and thereafter, a duty to hold all such confidential or proprietary information in the strictest confidence and not to disclose it to any person, firm or corporation or to use it except as necessary in carrying out Consultant's services for the Company consistent with the Company's agreement with such third party.

c. Consultant agrees that all copyrightable material, notes, records, drawings, designs, inventions, improvements, developments, discoveries and trade secrets pertaining to the design and performance of the Company's technology (collectively, "Inventions") conceived, made or discovered by Consultant, solely or in collaboration with others, during the period of this Agreement which relate in any manner to the business of the Company that Consultant may be directed to undertake, investigate or experiment with, or which Consultant may become associated with in work, investigation or experimentation in the line of business of Company in performing Consultant's services hereunder, are the sole property of the Company. In addition, any Inventions which constitute copyrightable subject matter shall be considered "works made for hire" as that term is defined in the United States Copyright Act. Consultant further agrees to assign (or cause to be assigned) and does hereby assign fully to the Company all such Inventions and any copyrights, patents, mask work rights or other intellectual property rights relating thereto. If unrelated to the design or performance of the Company's technology, any copyrightable material, notes, records, drawings, designs, inventions, improvements, developments, discoveries and trade secrets conceived, made or discovered by Consultant, solely or in collaboration with others, during the period of this Agreement, shall not be property of the Company.

d. Consultant agrees to assist Company, or its designee, at the Company's expense, in every proper way to secure the Company's rights in the Inventions and any copyrights, patents, mask work rights or other intellectual property rights relating thereto in any and all countries, including the disclosure to the Company of all pertinent information and data with respect thereto, the execution of all applications, specifications, oaths, assignments and all other instruments which the Company shall deem necessary in order to apply for and obtain such rights and in order to assign and convey to the Company, its successors, assigns and nominees the sole and exclusive rights, title and interest in and to such Inventions, and any copyrights, patents, mask work rights or other intellectual property rights relating thereto. Consultant further agrees that Consultant's obligation to execute or cause to be executed, when it is in Consultant's power to do so, any such instrument or papers shall continue after the termination of this Agreement.

e. Consultant agrees that if in the course of performing Consultant's services, Consultant incorporates into any Invention developed hereunder any invention, improvement, development, concept, discovery or other proprietary information owned by Consultant or in which Consultant has an interest, the Company is hereby granted and shall have a nonexclusive, royalty-free, perpetual, irrevocable, worldwide license to make, have made, modify, use and sell such item as part of or in connection with such Invention.

f. Consultant agrees that if the Company is unable because of Consultant's unavailability, dissolution, mental or physical incapacity, or for any other reason, to secure Consultant's signature to apply for or to pursue any application for any United States or foreign patents or mask work or copyright registrations covering the Inventions assigned to the Company above, then Consultant hereby irrevocably designates and appoints the Company and its duly authorized officers and agents as Consultant's agent and attorney in fact, to act for and in Consultant's behalf and stead to execute and file any such applications and to do all other lawfully permitted acts to further the prosecution and issuance of patents, copyright and mask work registrations thereon with the same legal force and effect as if executed by Consultant.

5. **Return of Materials.** Any materials or documents which have been furnished by one party to the other will be promptly returned, accompanied by all copies of such documentation after the consulting relationship has ended.

6. **Miscellaneous.** This Agreement shall be binding upon and for the benefit of the undersigned parties, their successors and assigns, provided that Confidential Information may not be assigned without consent of the disclosing party. Failure to enforce any provision of this Agreement shall not constitute a waiver of any term hereof.

7. **Governing Law and Jurisdiction.** This Agreement shall be governed by and construed under the laws of the State of California. The federal and state courts within the State of California shall have exclusive jurisdiction to adjudicate any dispute arising out of this Agreement.

8. **Term.** This Agreement shall survive until such time as all Confidential Information disclosed hereunder becomes publicly known and made generally available through no action or inaction of the Consultant, or five years have elapsed, whichever comes first.

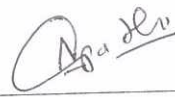
9. **Remedies.** Each party agrees that its obligations hereunder are necessary and reasonable in order to protect the other party and the other party's business, and expressly agrees that monetary damages would be inadequate to compensate the other party for any breach of any covenant or agreement set forth herein. Accordingly, each party agrees and acknowledges that any such violation or threatened violation will cause irreparable injury to the other party and that, in addition to any other remedies that may be available, in law, in equity or otherwise, the other party shall be entitled to obtain injunctive relief against the threatened breach of this Agreement or the continuation of any such breach, without the necessity of proving actual damages.

"COMPANY"

JUNIPER NETWORKS, INC.

By: \_\_\_\_\_  
Title: \_\_\_\_\_

"CONSULTANT"

By:   
Ashutosh Tripathi



## JUNIPER NETWORKS, INC

### CONTRACT WORKERS, VENDORS, CONSULTANTS AND INDEPENDENT CONTRACTORS CODE OF CONDUCT

The information contained in this Code is not a comprehensive, full or complete explanation of all of the policies, laws and regulations that may apply to you as a contract worker, vendor, consultant or independent contractor of Juniper. In the event that you discover a conflict of interest or events of a questionable, fraudulent or illegal nature, that are, or may be, in violation of the guidelines set forth in this Code, you should report the matter immediately to a member of Juniper's Concerns Committee or directly to a member of the Audit Committee of the Board of Directors, whose contact information can be found on Juniper's intranet site. You may also report the matter on a confidential (and, at your choice, anonymous) basis through Juniper's Ethics Helpline or by calling them toll-free at + 1 (888) 475-8388. No discrimination or retaliation against any person who, in good faith, reports such concerns will be tolerated. Any violation of this Code will result in disciplinary action up to and including termination of your status as a Juniper contract worker, vendor, consultant or independent contractor.

During the course of performing of services for Juniper:

1. Do not bring weapons, or anything that could be construed as a weapon, to a Juniper facility.
2. Do not engage in physical violence or verbal abuse.
3. Do not perform services for Juniper while under the influence of any substance, including drugs or alcohol, which prevents you from providing services safely and effectively.
4. Follow Juniper policies with respect to your physical access to Juniper sites.
5. Care for computer or other equipment provided by Juniper, maintain its security and use it responsibly for Juniper's business purposes. Incidental use of the equipment for personal reasons should be kept to a minimum and must not interfere with Juniper's business or harm Juniper's reputation. If such equipment is used outside of Juniper's premises, take precautions to protect it (and information of Juniper and its customers) from theft, damage, misuse and destruction. All such equipment and any information contained in it must remain fully accessible to Juniper and remains Juniper property.
6. Do not engage in any type of harassment or discrimination including, but not limited to, harassment of a sexual, religious or gender-based nature.
7. Maintain accurate time reports, expense accounts and other personal records related to services you provide to Juniper.
8. Avoid conflicts of interest. Do not engage in any activity that would interfere with your job performance or responsibilities. You must disclose to Juniper any interest you have that may conflict with Juniper's

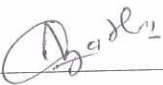
business or that may be perceived as something that could compromise your responsibilities or ability to make impartial and objective decisions related to the services you are providing to Juniper.

9. Do not, under any circumstances while acting on behalf of Juniper, offer to pay, pay, or issue authorization to pay any money, gift, kickback or anything of value to customers, vendors, employees, government officials, etc. that is or could be perceived as intended, directly or indirectly, to improperly influence any business decision, any act or failure to act, any commission of fraud, or opportunity for the commission of any fraud or obtain any unfair competitive advantage or which would violate federal or state and local laws or regulations, including but not limited to the Foreign Corrupt Practices Act ("FCPA") and the U. S. Federal Procurement Integrity Act.. You must fully comply with any rules regarding tender and bid processes. You may not offer employment to foreign officials if doing so would violate local laws.
10. Exercise no control over Juniper funds and strictly follow Juniper procedures and policies for maintaining books, records and accounts, carrying out and reporting business transactions, obtaining the appropriate authorization from management for those transactions and retaining appropriate documentation.
11. In the event that you come into possession of significant, sensitive material information about Juniper or another company with which Juniper either has or is contemplating a relationship, you may not engage in insider trading by buying or selling securities yourself or passing on the information to others to enable them to profit or for them to profit on your behalf.
12. Do not make any written or oral representations, commitments or agreements on Juniper's behalf (including product feature commitments) without prior written approval from Juniper.
13. Comply strictly with all applicable export and import laws and regulations and not export, re-export, transfer, divert, release, import or disclose any Juniper products or any direct product thereof, technical data relating to such products or Juniper confidential information to any other person or entity (nor shall you make any use thereof) except under license or as otherwise permitted under such laws and regulations.
14. Comply strictly with any confidentiality or non-disclosure obligations you have with Juniper and others.
15. Report to Juniper's General Counsel alleged improper or illegal conduct by Juniper employees.
16. Maintain a process by which employees may communicate a grievance, have a documented policy that details processes for remediation of abuses, including fair treatment of employees, and have a policy of non-retaliation for raising grievances.



17. Juniper supports freely chosen employment, child labor avoidance, reasonable working hours, wages and benefits, humane treatment, nondiscrimination and freedom of association. Juniper requires that you not engage in human trafficking and involuntary servitude of any type and that you have an effective program to promote and ensure that and the humane treatment of workers.

NAME: Ashutosh Tripathi DATE: 29/03/2019

SIGNATURE: 

For purposes of this document, the term "Contractor" shall mean any contract worker, vendor, consultant or independent contractor, and their employees, agents or subcontractors providing goods or services to Juniper Networks, Inc., its subsidiaries and/or affiliates ("Juniper Networks").

Contractors providing goods or services to Juniper Networks are fully responsible for the safe performance of all work performed by or on behalf of the Contractor. Contractor must prove adequate protection for the health, safety and welfare of Juniper Networks employees and the general public as well as for their own employees, subcontractors, and agents.

Contractor shall maintain good order at all times among their employees, subcontractors and agents and shall employ or contract with only qualified, responsible personnel capable and qualified of performing the work assigned to them.

Before bringing any chemical, substance or other material onto Juniper Networks premises, Contractor will provide all applicable safety data sheets to Juniper Networks Safety and Security Department for review and approval. All chemical, substance or other material brought onto Juniper Networks premises shall be clearly labeled and stored and disposed of per local regulations. In turn, Contractor is hereby advised that Juniper Networks uses limited hazardous materials in its own R&D and maintenance operations. Contractor may review Juniper Networks hazard communication program and hazardous materials inventory through a request to their Juniper Networks representative or directly to the Safety and Security Department.

Contractor acknowledges that Juniper Networks Safety and Security Department is to be advised of ALL emergency situations. To notify Juniper Networks Safety and Security Department and activate an emergency response, dial the emergency telephone number and stay on the line.

**Americas: +1 408 745 2911**

**Europe, the Middle East and Africa (EMEA): +31 20 7125794**

**Asia Pacific (APAC): +91 80 61214500**

Contractor understands and acknowledges that the following list of safety and security rules is not intended to cover each and every safety and security situation. Contractor will exercise good judgment in all safety and security matters and is aware that there may be other more specific safety and security procedures that may apply to their assignment at Juniper Networks.

Contractor acknowledges that disregard or violation of Juniper Networks safety and security rules may result in the termination of any existing contract with Juniper Networks.



---

### **Safety and Security Rules:**

1. Contractor shall support Juniper Networks Environmental, Health, Safety and Security Commitment: comply with applicable legal and other requirements that relate to the environmental aspects and health and safety hazards; prevent pollution, injury and ill health; and commit to continual improvement in performance.
2. Contractor is required to sign-in and obtain proper identification at the Juniper Networks lobby before commencing work on Juniper Networks premises and will prominently wear the Juniper Networks issued identification badge at all times while on Juniper Networks premises.
3. Contractor will go directly to his/her designated work area when arriving at Juniper Networks.
4. While on Juniper Networks premises, Contractor shall remain in his/her designated work area, except for meal and rest breaks, or when otherwise authorized by a Juniper Networks representative.
5. Unsafe work conditions will be reported by Contractor immediately to his/her Juniper Networks contact/supervisor, and/or to the Juniper Networks Safety and Security Department.
6. Contractor shall provide and use personal protective equipment as required by OSHA and other regulatory agencies.
7. Smoking is not permitted in any Juniper Networks building and is only permitted in designated smoking areas.
8. No alcoholic beverages or drugs are permitted on Juniper Networks premises, unless previously approved by an authorized Juniper Networks representative, and no person under the influence of drugs or alcohol will be permitted on Juniper Networks premises.
9. No firearms or other weapons are permitted on Juniper Networks premises.
10. No fighting or "horseplay" will be tolerated at any time on Juniper Networks premises.
11. Fire protection and prevention practices, including the clearance of passage aisles and doorways, fire extinguishers, and electrical panels, and proper storage of flammable or combustible materials, must be observed by Contractor at all times.
12. Contractor shall not operate or disturb any equipment, machinery, valves or electrical controls unless authorized by Juniper Networks to do so.
13. Guards and safety devices installed over a point of operation, moving parts, or electrical connections must be in place at all times with respect to equipment or tools utilized by Contractor.



14. All hotwork must be pre-approved and a hotwork permit must be issued by a Juniper Networks representative.
15. Adequate warning signs and barricades must be placed by Contractor at strategic locations where there is a concentration of work or hazardous operation.
16. Good housekeeping must be maintained, and work areas must be kept clear and orderly by Contractor.

### Acknowledgment of Receipt and Understanding:

In addition to the above, I acknowledge that I have received the following documents:

- **Your New ID Badge Rules**
- **Business Partner Code of Conduct**
- **Environmental, Health, Safety and Security Commitment**
- **Information Security Policy**
- **Acceptable Use Policy**

I have read and understand these documents, and will comply with the contents and directives set forth herein. I will provide copies of these documents to any of my employees, agents, or subcontractors who will be on Juniper Networks premises or accessing Juniper's systems.

Signature:  Date: 29/03/2019

Print

Name: Ashutosh Tripathi



## Vendor Service Provider Access Request Form

Individuals requiring physical badge access to Juniper facilities and/or Juniper IT systems (Juniper's Network) must complete all parts of this form and the ones listed below in order to gain access.

A valid purchase order is required prior to granting access for VSP personnel. Consult the Purchasing Department for guidance on establishing purchase orders. Vendor personnel require Contract Manager Approval.

Personnel who require background check processing are authorized interim temporary badge access for 5 working days. Personnel whose background reports do not meet Juniper standards agree to surrender access credentials on request from Juniper.

### Additional On-boarding Documents and Instructions

Documents to be filled out by Juniper Reporting Manager/Admin:

- VSP Access Request Form Approvals

Documents to be filled out and signed by individual:

- Contractor Confidential Information and Invention Assignment Agreement (CCIIAA) or Non-Disclosure Agreement (for specific locations only)
- Non-Employee Code of Conduct
- Safety & Security Rules

Documents to be reviewed, but not signed, by individual:

- Information Security Acceptable Use Policy
- Environmental, Health, Safety and Security Commitment

Documents for vendor HR or personnel who will review the background check results of individual (for specific locations only):

- Background Check Guidelines and Certification Form
- Example Process: Review of Results to the Juniper Networks Background Check Guidelines

To be completed by VSP Admin:

Date reviewed and entered into PeopleSoft: \_\_\_\_\_

Processed by VSP admin (name): \_\_\_\_\_



Vendor (New Individual), please provide information below:

Have you previously worked for Juniper Networks as an employee or contractor? ☐ YES / ☒ NO

If yes, please provide your previous Juniper ID number (if known): \_\_\_\_\_

Vendor Company: Talentica Software (India) Pvt. Ltd.

First Name: Ashutosh Last Name: Tripathi

Preferred First Name: Ashutosh Preferred Last Name: Tripathi

Email: ashutosh.tripathi@talentica.com Telephone Number: +91-8600 998631

Emergency Contact Name: Divya Tripathi

Emergency Contact Telephone: +91-7276647609

- To help Juniper determine whether it may need to obtain an export license before it can disclose controlled technology to you, please indicate whether you are a citizen of any of the following countries: Cuba, Iran, North Korea, Sudan, Syria. ☐ YES / ☒ NO

- If you answered "Yes" to the preceding question, did you later obtain citizenship or permanent residency status in any country NOT in that list of countries? ☐ YES / ☐ NO

Juniper Reporting Managers or Admins Approval:

Person Start Date: \_\_\_\_\_ Person End Date: \_\_\_\_\_

Contract End Date: \_\_\_\_\_ SAP Department Number: \_\_\_\_\_

Job Code: \_\_\_\_\_

Reporting Job Location (City/State, or Country): \_\_\_\_\_

Reporting Juniper Manager Name: \_\_\_\_\_

Reporting Juniper Manager EMP ID #: \_\_\_\_\_

A valid purchase order is required PRIOR to granting access. Exceptions to the PO requirement must be explained and documented; additional approvals may be required. You must also confirm that the worker will NOT be paid via money from any "Market Development Funds (MDF)."

Do you have a valid purchase order? ☐ YES / ☐ NO

Purchase Order # \_\_\_\_\_

If no PO is available, please provide a valid reason why: