

**DATA USAGE AND PROTECTION AGREEMENT- DATA CONTROLLER TERMS  
(Worldwide – One-Way)**

This DATA USAGE AND PROTECTION AGREEMENT (the “Agreement”) by and between Cisco Systems, Inc. whose registered office is at [*INSERT REGISTERED ADDRESS*] and its Affiliates (“Cisco”), and \_\_\_\_\_ a \_\_\_\_\_ [corporation] having its principal place of business at \_\_\_\_\_ (“Vendor”), is entered into as of the date last written below (“the Effective Date”).

This Agreement is the complete agreement between the parties concerning the subject matter of this Agreement and replaces any prior oral or written communications between the parties. There are no conditions, understandings, agreements, representations, or warranties expressed or implied, that are not specified herein. This Agreement is drafted in the English language. If this Agreement is translated into any other language, the English language text shall prevail. This Agreement may only be modified by a written document executed by the parties hereto.

Vendor, by enrolling as a Cisco supplier, confirms that it has read, understands and expressly approves the following clauses: 5.1, 5.2, 5.3, 7.1, 8.1, 10.1, 11.1, 14.5 and 14.8, in addition to the other terms and conditions of this Agreement.

The parties have caused this Agreement to be duly executed. Each party warrants and represents that its respective signatories whose signatures appear below are on the date of signature authorized to execute this Agreement.

\_\_\_\_\_  
 (“Vendor”)

\_\_\_\_\_  
 (“Cisco”)

\_\_\_\_\_  
 Authorized Signature

\_\_\_\_\_  
 Authorized Signature

\_\_\_\_\_  
 Name

\_\_\_\_\_  
 Name

\_\_\_\_\_  
 Date

\_\_\_\_\_  
 Date

## **DATA USAGE AND PROTECTION AGREEMENT TERMS AND CONDITIONS**

### **1. RECITALS**

According to the terms and conditions of this Agreement, Cisco is willing to provide to Vendor and Vendor may have access to or needs to access and receive certain Cisco Data as defined below.

### **2. DEFINITIONS**

- 2.1 "Affiliates" means any entity that directly or indirectly controls, is controlled by, or is under common control with, another entity, for so long as such control exists. In the case of companies and corporations, "control" and "controlled" means beneficial ownership of more than fifty percent of the voting stock, shares, interest or equity in an entity. In the case of any other legal entity, "control" and "controlled" shall exist through the ability to directly or indirectly control the management and/or business of the legal entity.
- 2.2 "Cardholder Data" means a cardholder's name, full account number, expiration date or the three-digit or four-digit security number printed on the front or back of a payment card.
- 2.3 "Cisco Data" means any Personal Data (whether confidential or not) made available to Vendor by Cisco or which Vendor accesses and processes on Cisco's behalf.
- 2.4 "Data Protection Laws" means the data protection and privacy laws of each country where a Cisco entity that is legally responsible for any of the Cisco Data is established and those of each country where any of the Cisco Data is collected or otherwise processed, including without limitation such laws and regulations that implement the European Data Protection Directive and the Privacy and Electronic Communications Directive (2002/58/EC) in the European Economic Area ("EEA") and any applicable guidelines and codes issued by a competent data protection authority, or other competent governmental body or agency, in respect of such laws.
- 2.5 "European Data Protection Directive" shall mean the European Data Protection Directive (95/46/EC).
- 2.6 The terms "process" and "Personal Data", or their equivalent, shall have their respective meanings under the Data Protection Laws. If any term referred to in this Clause 2.6 is not expressly defined and has no equivalent under the Data Protection Laws, it shall be given its meaning under the European Data Protection Directive. For purposes of this Agreement, "process" shall be deemed to include access to Personal Data.
- 2.7 The terms and conditions of this Agreement shall apply to all processing of Cisco Data performed by the Vendor in connection with any commercial arrangements it has with Cisco, notwithstanding any provision to the contrary in any other

agreement, order confirmation, specification, or other commercial document entered into on or before the date of this Agreement.

### **3. COMPLIANCE WITH LAWS AND REGULATIONS**

- 3.1 Vendor shall at all times comply with the Data Protection Laws and in the event and to the extent that the Data Protection Laws impose stricter obligations on the Vendor than under this Agreement, the Data Protection Laws shall prevail.
- 3.2 Vendor shall provide all information and co-operation regarding the processing of Cisco Data as Cisco may reasonably require to enable Cisco to comply with the Data Protection Laws.
- 3.3 Vendor shall nominate a representative within its organization with responsibility to respond to all of Cisco's queries regarding the processing of Cisco Data and Vendor shall ensure that it responds to all such queries promptly.
- 3.4 Where Vendor receives, processes, transmits or stores any Cardholder Data on behalf of Cisco, Vendor represents and warrants that information security procedures, processes and systems will at all times meet or exceed all applicable information security laws, standards, rules and requirements related to the collection, storage, processing and transmission of Credit Card Information, including those established by applicable governmental regulatory agencies, the Payment Card Industry ("PCI"), all applicable Networks, and any written standards provided by Cisco's information security group to Vendor from time to time (all the foregoing collectively "PCI Compliance Standards"). On the effective date of this Agreement and annually thereafter, or upon Cisco's request, Vendor will provide written evidence from each Network for which Vendor collects, stores, processes and/or transmits Cardholder Data evidencing Vendor's compliance with the PCI Compliance Standards and any applicable rules and requirements of the Network. As used herein, "Network" means credit, debit, payment and card authorization or processing networks, including without limitation, VISA, MasterCard, American Express, DiscoverCard and JCB International. Under no circumstances will Vendor provide Cisco or any Cisco employees with any Cardholder Data or access to Cardholder Data.

### **4. SECURITY AND MANAGEMENT OF CISCO DATA**

- 4.1 Where Vendor is processing Cisco Data, Vendor undertakes, represents and warrants:
  - 4.1.1 to implement and maintain all appropriate technical, physical and organisational security and confidentiality measures as required by the Data Protection Laws and as necessary to protect against unauthorised or unlawful processing of Cisco Data and against accidental loss, alteration, disclosure or destruction of, misuse of, or damage to, Cisco Data held or processed by or on behalf of Vendor, and to take all reasonable steps to ensure the reliability of any of Vendor's staff who have access to or are responsible for the processing of Cisco Data including, where required by the Data Protection Laws, appointing and instructing such staff in writing to process Cisco Data only under the authority and responsibility

of Vendor;

- 4.1.2 to process Cisco Data only as necessary to fulfil its contractual obligations to Cisco and, where the Vendor is processing Cisco Data on behalf of Cisco, only under the instructions of Cisco;
- 4.1.3 not to do anything in relation to the Cisco Data which may put Cisco in breach of any Data Protection Laws;
- 4.1.4 to document, implement and maintain such processes and systems as are necessary to process Cisco Data in compliance with all Data Protection Laws (including but not limited to the management of "opt-out," "opt-in" and "unsubscribe" requests from individuals and the exercise of any of such individuals' other rights under the Data Protection Laws);
- 4.1.5 only as required by the Data Protection Laws and where the Vendor is processing Cisco Data on behalf of Cisco, to ensure all documentation referred to in Clause 4.1.4 which relates to data security shall identify: (i) the Cisco entity(ies) legally responsible for the relevant Cisco Data; (ii) the processing undertaken by the Vendor on behalf of Cisco; and (iii) any databases/systems used by the Vendor to process Cisco Data on behalf of Cisco;
- 4.1.6 to assist Cisco promptly with all subject access, rectification, cancellation, objection and other data protection related requests, or inquires and complaints which may be received from individuals and to notify Cisco promptly if Vendor receives any such request, inquiry or complaint;
- 4.1.7 where the Vendor is processing Cisco Data on behalf of Cisco, the Vendor shall not respond to any requests, inquires or complaints referred to in Clause 4.1.6 without, and in accordance with, the prior written approval of Cisco at Cisco's sole discretion unless required by applicable law;
- 4.1.8 not to disclose Cisco Data, or any information regarding the care, custody or processing of Cisco Data, to any third party in any circumstances other than at the specific request and authorisation of Cisco or as otherwise permitted by this Agreement unless required by applicable law; and
- 4.1.9 to promptly carry out any request from Cisco requiring Vendor to amend, transfer or delete, or to provide Cisco with a copy of, in Cisco's preferred format, the Cisco Data or any part of the Cisco Data.

## **5. SUB-PROCESSORS**

- 5.1 Vendor shall not sub-contract or otherwise delegate all or any part of its processing of Cisco Data to any other person or entity ("Sub-Processor") without Cisco's prior written consent at Cisco's sole discretion.

- 5.2 Prior to seeking Cisco's consent, Vendor shall provide Cisco with full details of the proposed Sub-Processor's involvement including but not limited to the identity of the Sub-Processor, its data security record, the location of its processing facilities, a description of the access to Cisco Data proposed and any other information Cisco may reasonably request in order to assess the risks involved in allowing the Sub-Processor to process Cisco Data.
- 5.3 Without prejudice to clause 6, Cisco may as a condition of providing its consent to any proposed sub-processing:
- 5.3.1 require Vendor to enter into a written agreement with the Sub-Processor containing equivalent terms to this Agreement (provided that Vendor shall not be entitled to permit the Sub-Processor to further sub-contract or otherwise delegate all or any part of the Sub-Processor's processing without Cisco's prior written consent at Cisco's sole discretion) and which expressly provides Cisco with third party beneficiary rights to enforce such terms; and/or
- 5.3.2 require Vendor to procure that the Sub-Processor enters into a data processing agreement with Cisco directly.

## 6. EXPORT

- 6.1 Vendor undertakes, represents and warrants not to transfer, process, nor to permit any Sub-Processor to transfer, process Cisco Data outside of the jurisdiction in which the Cisco Data has been made available to the Vendor by Cisco or, where Cisco Data has been made available by Cisco to the Vendor inside of the EEA, outside of the EEA (in both cases, such processing being an "Export Of Cisco Data") except:
- 6.1.1 with Cisco's prior written consent at Cisco's sole discretion; or
- 6.1.2 where the transferring or processing will take place exclusively in a state or territory and under circumstances approved from time to time by the European Commission as "adequate" under Article 25(6) of the European Data Protection Directive (95/46/EC), which shall include the EU-US Safe Harbor arrangement provided that Vendor's EU-US Safe Harbor certification is up to date and adequate and appropriate to cover Vendor's transferring or processing of Cisco Data and Vendor shall not make any onward transfers of Cisco Data without Cisco's prior written consent at Cisco's sole discretion.
- 6.3 Prior to any proposed Export Of Cisco Data, Cisco may require Vendor to execute such additional terms and to take such further steps as Cisco shall reasonably require in order to legitimise the Export Of Cisco Data, including without limitation executing the Standard Contract Clauses for the transfer of Personal Information to third countries under Directive 95/46/EC contained in the Annex to Commission Decisions 2001/497/EC, 2002/16/EC, 2004/915/EC and 2010/87/EU (as applicable), and to fulfil, or to assist Cisco to fulfil, such regulatory requirements, including making notifications and obtaining such approvals as are necessary at Vendor's cost.

## **7. INDEMNIFICATION**

- 7.1 Vendor agrees that it shall be responsible for all acts and omissions in respect of the processing of Cisco Data, including the acts and omissions of its employees, agents, independent contractors and Sub-Processors (each a “Representative”). Vendor agrees to indemnify and hold harmless and, upon Cisco's request, to defend Cisco and its directors, officers, employees, shareholders and agents from and against any and all third party claims of damages, liabilities, expenses, claims, fines and losses of any type, including but not limited to reasonable attorneys' fees, in connection with or arising out of, in whole or in part, Vendor's and/or its Representative's breach of this Agreement.

## **8. DISCLAIMER**

- 8.1 CISCO DATA IS PROVIDED “AS IS” WITH ALL FAULTS. IN NO EVENT SHALL CISCO BE LIABLE TO VENDOR FOR THE INACCURACY OR INCOMPLETENESS OF THE CISCO DATA.

## **9. AUDIT AND REPORTING REQUIREMENTS**

- 9.1 Cisco and its agents, consultants, contractors and representatives shall have the right on reasonable notice from Cisco to attend Vendor's facilities to inspect and audit Vendor's storage or processing of Cisco Data to ensure compliance with this Agreement, including in particular, with respect to data security. In the event that an inspection and audit of Vendor's facilities finds that Vendor is not in compliance with this Agreement, Vendor shall, without prejudice to any other rights or remedies Cisco may have under this Agreement, take all reasonable steps to promptly remedy any breach identified by the inspection and audit, or provide Cisco with a detailed report as to why such breach cannot be remedied, and to pay Cisco's reasonable costs of such an inspection and audit.
- 9.2 Vendor will notify Cisco immediately upon discovery of (i) any lost or altered Personal Data collected, held or processed by Vendor on Cisco's behalf, (ii) any breaches of its information security systems or (iii) attempts to penetrate such systems that compromise or reasonably could compromise Personal Data and will coordinate with Cisco's security personnel in connection with the investigation and remediation of the security breach. Vendor will maintain records of any known or suspected security breaches in accordance with commercially accepted industry practices and will make such records reasonably available to Cisco and its affected customers upon request. Except as required by applicable law, Vendor agrees that it will not inform any third party of any such security breach without Cisco's prior written consent. If such disclosure is required by law, Vendor will work with Cisco regarding the content of the disclosure to minimize any potential adverse impact upon Cisco and its customers. Vendor will bear the cost of reproduction or any other remedial steps necessary or advisable to address the security breach.

## **10. WAIVER OF CONSEQUENTIAL DAMAGES**

- 10.1 IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL OR STATUTORY

DAMAGES, INCLUDING ANY LOST DATA OR LOST PROFITS, RELATED TO THIS AGREEMENT.

## **11. LIMITATION OF LIABILITY**

- 11.1 TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL CISCO'S CUMULATIVE LIABILITY IN CONNECTION WITH THIS AGREEMENT WHETHER IN CONTRACT OR IN TORT OR OTHERWISE, EXCEED DIRECT DAMAGES IN AN AMOUNT OF \$15,000 (US).

## **12. TERM**

- 12.1 This Agreement shall continue from the Effective Date until terminated by Cisco upon thirty (30) days' written notice to Vendor of its intent to terminate this Agreement. Notwithstanding such termination, Clauses 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, and 14 shall survive termination or expiration of this Agreement.

## **13. RETURN OF CISCO DATA**

- 13.1 Upon termination or expiration of this Agreement or upon written request by Cisco, Vendor shall: (i) immediately cease processing the Cisco Data; and (ii) return to Cisco, or at Cisco's option destroy, the Cisco Data and all copies, notes or extracts thereof and including but not limited to hardware and software product registration cards, change of address requests, do-not-solicit requests, direct marketing program responses, fulfilment program information, and any other information captured from *ad hoc* programs, within seven (7) business days of the date of termination or expiration of this Agreement or of receipt of request. Upon the request of Cisco, Vendor shall also confirm in writing that Vendor has complied with the obligations set forth in this clause.

## **14. GENERAL**

- 14.1 The Vendor acknowledges that monetary remedies may be inadequate to protect Cisco Data and that injunctive relief may be appropriate to protect such Cisco Data.
- 14.2 The parties hereto are independent contractors.
- 14.3 Neither party shall be liable to the other for delays or failures in performance resulting from causes beyond the reasonable control of that party, including, but not limited to, acts of God, labor disputes or disturbances, material shortages or rationing, riots, acts of war, governmental regulations, communication or utility failures, or casualties.
- 14.4 Unless otherwise expressly provided under this Agreement, no provisions of this Agreement are intended or shall be construed to confer upon or give to any person or entity other than Cisco and Vendor any rights, remedies or other benefits under or by reason of this Agreement.

- 14.5 Unless otherwise expressly provided under this Agreement, a party may not assign this Agreement or assign its rights or delegate its obligations hereunder, either in whole or in part, whether by operation of law or otherwise, without the prior written consent of the other. Any attempt at such an assignment or delegation without the other's written consent will be void. The rights and liabilities of the parties under this Agreement will bind and inure to the benefit of the parties' respective successors and permitted assigns. For purposes of this clause, a twenty percent (20%) change in control of Vendor shall constitute an assignment.
- 14.6 Failure by either party to enforce any provision of this Agreement will not be deemed a waiver of future enforcement of that or any other provision. Any waiver, amendment, variation or other modification of any provision of this Agreement will be effective only if in writing and signed by the parties.
- 14.7 If any term of this Agreement shall be held to be illegal or unenforceable by a court of competent jurisdiction, the remaining terms shall remain in full force and effect.
- 14.8 The parties specifically disclaim the UN Convention on Contracts for the International Sale of Goods. This Agreement and any action related thereto shall be governed, controlled, interpreted and defined by and under the laws specified below, and is subject to the exclusive jurisdiction of the courts specified below:

<b>Principal place/country location of business headquarters of the Vendor</b>	<b>Governing Laws</b>	<b>Courts Having Jurisdiction</b>
<b>(as specified at the top of this Agreement)</b>		
A country within the European Economic Area (EEA), Europe, the Middle East or Africa, or Russia	England and Wales	England
A country within the Asia-Pacific Economic Cooperation (APEC) (excluding Russia, the United States of America and Canada)	State of Victoria, Australia	State of Victoria, Australia
All other countries	all applicable federal, state and local laws of the United States of America	California, United States of America