MASTER DATA PROTECTION AGREEMENT

This MASTER DATA PROTECTION AGREEMENT ("MDPA") is entered in to by and between Cisco Systems, Inc. whose registered office is at 170 West Tasman Drive, San Jose, California 95134 and its Affiliates ("Cisco"), and Customer and its Affiliates ("Customer"), (together "Parties").

This MDPA is governed by the terms of the applicable agreement entered into by and between the Parties for the supply of Products and/or Services by Cisco to Customer ("the Agreement"). In the event of a conflict between this MDPA, including any attachments herein, and the Agreement, the provisions of this MDPA will control but only with respect to the subject matter hereof.

In consideration of the mutual promises and covenants hereinafter contained and of other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

1.0 SCOPE OF AGREEMENT. This MDPA is comprised of these General Terms and the following Attachments A-D attached herein, which are incorporated by reference:

1. Attachment A INFORMATION SECURITY EXHIBIT
2. Attachment B DATA PROTECTION EXHIBIT
3. Attachment C *Reserved*
4. Attachment D STANDARD CONTRACTUAL CLAUSES
5. Attachment E GLOSSARY

GENERAL TERMS

2.0 LIMITATION AND EXCLUSION OF LIABILITY.

2.1 Nothing in this MDPA limits or excludes the liability of either Party to the other for: (i) bodily injury or death resulting directly from the negligence of the other Party; (ii) fraud or fraudulent misrepresentation; (iii) a Party's unauthorized use or disclosure of Protected Data in breach of its obligations in this MDPA; or (iv) any liability that cannot be limited or excluded under mandatory applicable law.

2.2 Subject to Section 2.3 below and Section 2.4 below, each Party's total aggregate liability is limited to: One million dollars (US$1,000,000).

2.3 Subject to Section 2.4 below, and notwithstanding anything else in this MDPA to the contrary, neither Party will be liable for any: (i) special, incidental, indirect or consequential damages; (ii) loss of any of the following: profits, revenue, business, anticipated savings, use of any product or service, opportunity, goodwill or reputation; (iii) lost or damaged data; or (iv) wasted expenditure (other than any expenditure necessarily incurred to discharge the innocent Party's duty or to mitigate its losses).

2.4 This limitation of liability applies whether the claims are contract, tort (including negligence), misrepresentation or otherwise. This limitation of liability is in the aggregate and not per incident.

3.0 WARRANTY DISCLAIMER. EXCEPT AS EXPRESSLY SET OUT IN THIS MDPA, ALL CONDITIONS, WARRANTIES AND REPRESENTATIONS, EXPRESS OR IMPLIED BY (I) STATUTE, (II) COMMON LAW OR (III) OTHERWISE, ARE EXCLUDED TO THE FULLEST EXTENT PERMITTED BY LAW.

4.0 MISCELLANEOUS.

4.1 Choice of Law.

4.1.1 If Customer's principal place of business is located in Europe, the Asia Pacific region (excluding Australia and Japan), the Middle East Africa, Russia and the Commonwealth of Independent States [CIS], or Eastern Europe, this MDPA and its validity, interpretation, and performance shall be governed by the laws of England without giving effect to principles of conflicts of laws. The Parties accept the exclusive jurisdiction of the English courts, provided that either party may bring an action before any court of appropriate jurisdiction for interim injunctive relief for protection of intellectual property rights and confidential information. The Parties specifically disclaim the UN Convention on Contracts for the International Sale of Goods and it shall not apply to the interpretation or enforcement of this MDPA.

4.1.2 If Customer's principal place of business is located in a jurisdiction other than those stated in Section 4.1.1 above, the validity, interpretation, and performance of this MDPA shall be governed by and construed under the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflicts of law. The Federal District Court, Northern District of California or the Superior Court of Santa Clara County, California shall have exclusive jurisdiction over any claim arising under this MDPA, provided that either Party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such Party's intellectual property or proprietary rights. The Parties specifically disclaim the UN Convention on Contracts for the International Sale of Goods and it shall not apply to the interpretation or enforcement of this MDPA.

4.2 Attorneys' Fees. In any suit or proceeding relating to this MDPA the prevailing Party will have the right to recover from the other its costs and reasonable fees and expenses of attorneys, accountants, and other professionals incurred in connection with the suit or proceeding, including costs, fees and expenses upon appeal, separately from and in addition to any other amount included in such judgment. This provision is intended to be severable from the other provisions of this MDPA, and shall survive expiration or termination and shall not be merged into any such judgment.

4.3 No Waiver. The waiver by either party of any right provided under this MDPA shall not constitute a subsequent or continuing waiver of such right or of any other right under this MDPA.

4.4 Assignment. Unless otherwise expressly provided under this MDPA, neither Party may assign this MDPA 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 Party. Any attempt at such an assignment or delegation without the other's Party's written consent will be void. The rights and liabilities of the parties under this MDPA will bind and inure to the benefit of the Parties' respective successors and permitted assigns. For purposes of this Section 4.4 (Assignment), a twenty percent (20%) change in control of a Party shall constitute an assignment.

4.5 Severability. If one or more terms of this MDPA become or are declared to be illegal or otherwise unenforceable by any court of competent jurisdiction, each such part or term shall be null and void and shall be deemed deleted from this MDPA. All remaining terms of this MDPA shall remain in full force and effect. However, if this paragraph is invoked and, as a result, the value of this MDPA is materially impaired for either Party, then the affected Party may terminate this MDPA by written notice with immediate effect.

4.6 Notices. All notices required or permitted under this MDPA shall be in writing. Notices will be deemed to have been given (i) one day after deposit with a commercial express courier specifying next day delivery; or (ii) two days for international courier packages specifying two-day delivery, with written verification of receipt. All communications shall be sent to the Parties' addresses shown on the first page of this MDPA or to such other address as may be designated from time to time by a Party by giving at least fourteen (14) days' written notice to the other Party.

4.7 Survival. The following sections shall survive the expiration or earlier termination of this MDPA: 2.0 (Limitation and Exclusion of Liability), 3.0 (Warranty Disclaimer), and 4.0 (Miscellaneous).

This MDPA is the complete agreement between the Parties concerning the subject matter of this MDPA and replaces any prior oral or written communications between the Parties. This MDPA is subject to the terms and conditions of the Agreement, including, but not limited to any limitations or exclusions of liability set forth in the Agreement. This MDPA, together with the Agreement, comprises the complete agreement between the Parties. There are no conditions, understandings, agreements, representations, or warranties expressed or implied, that are not specified herein. This MDPA may only be modified by a written document executed by the Parties hereto. The Parties, by signing below, confirm that they have read, understood, and expressly approve of the terms and conditions of this MDPA. Cisco's obligations under this MDPA will terminate when Cisco no longer holds, Processes, or otherwise has access to Protected Data.

The Parties have caused this MDPA 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 MDPA.

_____	_____
("Customer")	("Cisco")
_____	_____
Authorized Signature	Authorized Signature
_____	_____
Name	Name
_____	_____
Date	Date

ATTACHMENT A

INFORMATION SECURITY EXHIBIT

1. Scope

This Information Security Exhibit ("ISE") applies to the extent that Cisco Processes or has access to Protected Data in the Performance of its obligations to the Customer. This ISE outlines the information security requirements between Customer and Cisco and describes the technical and organizational security measures that shall be implemented by Cisco to secure Protected Data prior to the Performance of any Processing under the Agreement.

Unless otherwise stated, in the event of a conflict between the Agreement and this ISE, the terms of this ISE will control as it relates to the Processing of Protected Data.

All capitalized terms not defined in the Glossary have the meanings set forth in the Agreement.

2. General Security Practices

Cisco has implemented and shall maintain appropriate technical and organizational measures designed to protect Protected Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, procedures, and internal controls set forth in this ISE for its personnel, equipment, and facilities at Cisco's locations involved in Performing any part of the Agreement.

3. General Compliance

i. **Compliance**. Cisco shall document and implement processes and procedures to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security or other security requirements. Such processes and procedures shall be designed to provide appropriate security to protect Protected Data given the risk posed by the nature of the data Processed by Cisco. Cisco shall implement and operate information security in accordance with Cisco's own policies and procedures, which shall be no less strict than the information security requirements set forth in this ISE.

ii. **Protection of records**. Cisco shall implement appropriate procedures designed to protect records from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislative, regulatory, and contractual requirements.

iii. **Review of information security.** Cisco's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures) shall be reviewed at planned intervals or when significant changes occur by appropriate internal or external assessors.

iv. **Compliance with security policies and standards.** Cisco's management shall regularly review the compliance of information processing and procedures with the appropriate applicable security policies and standards.

v. **Technical compliance review.** Cisco shall regularly review information systems for compliance with Cisco's information security policies and standards.

vi. **Information Risk Management ("IRM").** Cisco shall implement and utilize an appropriate information risk management process to frame, assess, respond and monitor risk, consistent with

applicable contractual and legal obligations. Cisco is required to have a risk management framework and conduct periodic (i.e., at least annual) risk assessments of its environment and systems to understand the risks and apply appropriate controls to manage and mitigate such risks. Threat and vulnerability assessment must be periodically reviewed and prompt remediation actions taken where material weaknesses are found. Cisco will provide Customer with relevant summary reports and analysis upon written request, provided the disclosure of which would not violate Cisco's own information security policies, or mandatory applicable law.

4. Technical and Organizational Measures for Security

a. **Organization of Information Security**

i. **Security Ownership**. Cisco shall appoint one or more security officers responsible for coordinating and monitoring the security requirements and procedures. Such officers shall have the knowledge, experience, and authority to serve as the owner(s) of, with responsibility and accountability for, information security within the organization.

ii. **Security Roles and Responsibilities**. Cisco shall define and allocate information security responsibilities in accordance with Cisco's approved policies for information security. Such policies (or summaries thereof) shall be published and communicated to employees and relevant external parties required to comply with such policies.

iii. **Project Management**. Cisco shall address information security in project management to identify and appropriately address information security risks.

iv. **Risk Management**. Cisco shall have a risk management framework and conduct periodic (i.e., at least annual) risk assessment of its environment and systems to understand its risks and apply appropriate controls to manage and mitigate risks before Processing Protected Data.

b. **Human Resources Security**

i. **General**. Cisco shall ensure that its personnel are under a confidentiality agreement that includes the protection of Protected Data and shall provide adequate training about relevant privacy and security policies and procedures. Cisco shall further inform its personnel of possible consequences of breaching Cisco's security policies and procedures, which must include disciplinary action, including possible termination of employment for Cisco's employees and termination of contract or assignment for Representatives and temporary personnel.

ii. **Training**. Cisco personnel with access to Protected Data shall receive appropriate, annual periodic education and training regarding privacy and security procedures for services to aid in the prevention of unauthorized use (or inadvertent disclosure) of Protected Data and training regarding how to effectively respond to security incidents. Training shall be provided before Cisco personnel are granted access to Protected Data or begin providing services. Training shall be regularly reinforced through refresher training courses, emails, posters, notice boards, and other training and awareness materials.

iii. **Background Checks**. In addition to any other terms in the Agreement related to this subject matter, Cisco shall conduct criminal and other relevant background checks for its personnel in compliance with or mandatory applicable law and Cisco's policies.

c. **Personnel Access Controls**

i. **Access**.

A. Limited Use. Cisco understands and acknowledges that Customer may be granting Cisco access to sensitive and proprietary information and computer systems in order for Cisco to Perf-

orm its obligations to the Customer. Cisco will not (i) access the Protected Data or computer systems for any purpose other than as necessary to Perform its obligations to Customer; or (ii) use any system access information or log-in credentials to gain unauthorized access to Protected Data or Customer's systems, or to exceed the scope of any authorized access.

B. Authorization. Cisco shall restrict access to Protected Data and systems at all times solely to those Representatives whose access is necessary to Performing Cisco's obligations to the Customer.

C. Suspension or Termination of Access Rights. At Customer's reasonable request, Cisco shall promptly and without undue delay suspend or terminate the access rights to Protected Data and systems for any Cisco's personnel or its Representatives reasonably suspected of breaching any of the provisions of this ISE; and Cisco shall remove access rights of all employees and external party users upon suspension or termination of their employment, or engagement.

D. Information Classification. Cisco shall classify, categorize, and/or tag Protected Data to help identify it and to allow for access and use to be appropriately restricted.

ii. **Access Policy**. Cisco shall determine appropriate access control rules, rights, and restrictions for each specific user's roles towards their assets. Cisco shall maintain a record of security privileges of its personnel that have access to Protected Data, networks, and network services. Cisco shall restrict and tightly control the use of utility programs that might be capable of overriding system and application controls.

d. **Access Authorization**.

i. Cisco shall have user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to Customer's systems and networks. Cisco shall use an enterprise access control system that requires revalidation of its personnel by managers at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.

ii. Cisco shall maintain and update a record of personnel authorized to access systems that contain Protected Data and Cisco shall review users' access rights at regular intervals.

iii. For systems that process Protected Data, Cisco shall revalidate (or where appropriate, deactivate) access of users who change reporting structure and deactivate authentication credentials that have not been used for a period of time not to exceed six (6) months.

iv. Cisco shall restrict access to program source code and associated items such as software object code, designs, specifications, verification plans, and validation plans, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

e. **Network Design**. For systems that process Protected Data, Cisco shall have controls to avoid personnel assuming access rights beyond those that they have been assigned to gain unauthorized access to Protected Data.

f. **Least Privilege**. Cisco shall limit access to Protected Data to that personnel with Performance obligations and, to the extent technical support is needed, its personnel performing such technical support.

g. **Authentication**

i. Cisco shall use industry standard practices to identify and authenticate users who attempt to ac-

ces information systems. Where authentication mechanisms are based on passwords/PINs, Cisco shall require that the passwords/PINs are renewed and changed regularly, at least every 180 days.

ii. Where authentication mechanisms are based on passwords, Cisco shall require the password to conform to strong password control parameters (e.g., length, character complexity, and/or non-repeatability).

iii. Cisco shall ensure that de-activated or expired identifiers and log-in credentials are not granted to other individuals.

iv. Cisco shall monitor repeated failed attempts to gain access to the information system.

v. Cisco shall maintain industry standard procedures to deactivate log-in credentials that have been corrupted or inadvertently disclosed.

vi. Cisco shall use industry standard log-in credential protection practices, including practices designed to maintain the confidentiality and integrity of log-in credentials when they are assigned and distributed, and during storage (e.g., log-in credentials shall not be stored or shared in plain text). Such practices shall be designed to ensure strong, confidential log-in credentials.

h. **Physical and Environmental Security**

i. **Physical Access to Facilities**

A. Cisco shall limit access to facilities where systems that Process Protected Data are located to authorized individuals.

B. Security perimeters shall be defined and used to protect areas that contain both sensitive or critical information and information processing facilities.

C. Facilities shall be monitored and access-controlled at all times (24x7).

D. Access shall be controlled through key card and/or appropriate sign-in procedures for facilities with systems Processing Protected Data. Cisco must register personnel and require them to carry appropriate identification badges.

ii. **Physical Access to Equipment**. Cisco equipment used to process or store Protected Data shall be protected using industry standard processes to limit access to authorized individuals.

iii. **Protection from Disruptions**. Cisco shall implement appropriate measures designed to protect against loss of data due to power supply failure or line interference.

iv. **Clear Desk**. Cisco shall have policies requiring a “clean desk/clear screen” to prevent inadvertent disclosure of Protected Data.

i. **Operations Security**

i. **Operational Policy**. Cisco shall maintain written policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Protected Data and to its systems and networks. Cisco shall communicate its policies and requirements to all persons involved in the Processing of Protected Data. Cisco shall implement the appropriate management structure and control designed to ensure compliance with such policies and with or mandatory applicable law concerning the protection and Processing of Protected Data.

ii. **Security and Processing Controls**.

A. **Areas**. Cisco shall maintain, document, and implement standards and procedures to address the configuration, operation, and management of systems and networks and services that store or Process Protected Data.

B. **Standards and Procedures.** Such standards and procedures shall include: security controls, identification and patching of security vulnerabilities, change control process and procedures, and incident prevention, detection, remediation, and management.

iii. **Logging and Monitoring**. Cisco shall maintain logs of administrator and operator activity and data recovery events related to Protected Data.

j. **Communications Security and Data Transfer**

i. **Networks**. Cisco shall, at a minimum, use the following controls to secure its networks that access or Process Protected Data:

A. Network traffic shall pass through firewalls, which are monitored at all times. Cisco must implement intrusion prevention systems that allow traffic flowing through the firewalls and LAN to be logged and protected at all times.

B. Network devices used for administration must utilize industry standard cryptographic controls when Processing Protected Data.

C. Anti-spoofing filters and controls must be enabled on routers.

D. Network, application, and server authentication passwords are required to meet minimum complexity guidelines (at least 7 characters with at least 3 of the following four classes: upper case, lower case, numeral, special character) and be changed at least every 180 days; or utilize other strong log-in credentials (e.g., biometrics).

E. Initial user passwords are required to be changed at first log-on. Cisco shall have a policy prohibiting the sharing of user IDs, passwords, or other log-in credentials.

F. Firewalls must be deployed to protect the perimeter of Cisco's networks.

ii. **Virtual Private Networks ("VPN")**. When remote connectivity to the Customer's or Cisco's network is required for Processing of Protected Data:

A. Connections must be encrypted using industry standard cryptography (i.e., a minimum of 256-bit encryption).

B. Connections shall only be established using VPN servers.

C. The use of multi-factor authentication is required.

iii. **Data Transfer**. Cisco shall have formal transfer policies in place to protect the transfer of information through the use of all types of communication facilities that adhere to the requirements of this ISE. Such policies shall be designed to protect transferred information from unauthorized interception, copying, modification, corruption, routing and destruction.

k. **System Acquisition, Development, and Maintenance**

i. Security Requirements. Cisco shall adopt security requirements for the purchase, use, or deve-

lopment of information systems, including for application services delivered through public networks.

ii. **Development Requirements**. Cisco shall have policies for secure development, system engineering, and support. Cisco shall conduct appropriate tests for system security as part of acceptance testing processes. Cisco shall supervise and monitor the activity of outsourced system development.

l. **Penetration Testing and Vulnerability Scanning & Audit Reports**

i. **Testing.** Cisco will perform periodic penetration tests on its internet perimeter network. Audits will be conducted by Cisco's compliance team using industry recommended network security tools to identify vulnerability information. Upon written request from Customer, Cisco shall provide a Vulnerability & Penetration testing report at the organization level which may include an executive summary of the results and not the details of actual findings.

ii. **Audits.** Cisco shall respond promptly to and cooperate with reasonable requests by Customer for security audit, and testing reports. Customer shall treat the contents of and reports related to Cisco's security and certifications as Protected Data pursuant to the terms contained in this MDPA.

iii. **Remedial Action.** If any audit or penetration testing exercise referred to in Section 4(l)(ii), above reveals any deficiencies, weaknesses, or areas of non-compliance, Cisco shall promptly take such steps as may be required, in Cisco's reasonable discretion, to address material deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable given the circumstances.

iv. **Status of Remedial Action.** Upon request, Cisco shall keep Customer informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same, and shall certify to Customer as soon as may be practicable given the circumstances that all necessary remedial actions have been completed.

m. **Contractor Relationships**

i. **Policies**. Cisco shall have information security policies or procedures for its use of Representatives that impose requirements consistent with this ISE. Such policies shall be reviewed at planned intervals or if significant changes occur. Agreements with Representatives shall include requirements that are consistent with, or analogous to, this MDPA.

ii. **Monitoring**. Cisco shall monitor and audit service delivery by its Representatives and review its Representatives' security practices against the security requirements set forth in Cisco's agreements with such Representatives. Cisco shall manage changes in Representative services that may have an impact on security.

n. **Management of Information Security Incidents and Improvements**

i. **Responsibilities and Procedures**. Cisco shall establish procedures to ensure a quick, effective, and orderly response to Information Security Incidents.

ii. **Reporting Information Security Incident.** Cisco shall implement procedures for Information Security Incidents to be reported through appropriate management channels as quickly as reasonably possible. All employees and Representatives should be made aware of their responsibility to report Information Security Incidents as quickly as reasonably possible.

iii. **Reporting Information Security Weaknesses.** Cisco, employees, and Representatives are required to note and report any observed or suspected information security weaknesses in systems or services.

iv. **Assessment of and Decision on Information Security Events.** Cisco shall have an incident classification scale in place in order to decide whether a security event should be classified as an Information Security Incident. The classification scale should be based on the impact and extent of an incident.

v. **Response Process.** Cisco shall maintain a record of Information Security Incidents with a description of the incident, the effect of the incident, the name of the reporter and to whom the incident was reported, the procedure for rectifying the incident, and the remedial action taken to prevent future security incidents.

o. **Information Security Aspects of Business Continuity Management**

i. **Planning**. Cisco shall maintain emergency and contingency plans for the facilities where Cisco information systems that process Protected Data are located. Cisco shall verify the established and implemented information security continuity controls at regular intervals.

ii. **Data Recovery**. Cisco shall design redundant storage and procedures for recovering data in a manner sufficient to reconstruct Protected Data in its original state as found on the last recorded backup provided by the Customer.

5. Notification and Communication Obligations

a. **Notification**. Cisco shall without undue delay (i.e., within 48 hours from confirmation) notify Customer at:

Notification to Customer shall be sent to: [insert email address]

if any of the following events occur:

i. any unmitigated, material security vulnerability, or weakness of which Cisco has actual knowledge in (i) Customer's systems, or networks, or (ii) Cisco's systems or networks, that has compromised Protected Data;

ii. an Information Security Incident that compromises or is likely to compromise the security of Protected Data and weaken or impair business operations of the Customer;

iii. an Information Security Incident that negatively impacts the confidentiality, integrity, and availability of Protected Data that is Processed, stored, and transmitted using a computer; or

iv. known and willful failure or inability to maintain material compliance with requirements of this ISE and Applicable Laws.

b. **Cooperation**

Cisco shall: (i) respond promptly to any Customer reasonable requests for information, cooperation, and assistance, including to a Customer designated response center.

c. **Information Security Communication**

Except as required by mandatory applicable law or by existing applicable contractual obligations,

Cisco agrees that it will not inform any third party of any of the events described above in this Section referencing, or identifying the Customer, without Customer's prior written consent. Cisco shall fully cooperate with Customer and law enforcement authorities concerning any unauthorized access to Customer's systems or networks, or Protected Data. Such co-operation shall include the retention of all information and data within Cisco's possession, custody, or control that is directly related to any Information Security Incident. If disclosure is required by law, Cisco will work with Customer regarding the timing, content, and recipients of such disclosure. To the extent Cisco was at fault, Cisco will bear the cost of reproduction or any other remedial steps necessary to address the incident or compromise.

d. **Post-Incident**

Cisco shall reasonably cooperate with Customer in any post-incident investigation, remediation, and communication efforts.

ATTACHMENT B

DATA PROTECTION EXHIBIT

1. SCOPE

This Data Protection Exhibit ("DPE") outlines the terms and conditions with which the Parties must comply with respect to Processing Personal Data and applies to the extent that Cisco Processes or has access to Protected Data in the Performance of its obligations to the Customer.

2. DEFAULT STANDARDS

a. To the extent that Cisco Processes Special Categories of Data, the security measures referred to in this DPE shall also include, at a minimum (i) routine risk assessments of Cisco's information security program, (ii) regular testing and monitoring to measure and confirm the effectiveness of the information security program's key controls, systems, and procedures, and (iii) encryption of Special Categories of Data while during transmission (whether sent by e-mail, fax, or otherwise) and storage (including when stored on mobile devices, such as a portable computer, flash drive, PDA, or cellular telephone). If encryption is not feasible, Cisco shall not store Special Categories of Data on any unencrypted devices unless compensating controls are implemented. Cisco shall protect all Special Categories of Data stored on electronic databases, servers, or other forms of non-mobile devices against all reasonably anticipated forms of compromise by use of the safeguards contained in Attachment A (Information Security Exhibit).

b. In addition to the foregoing, to the extent Cisco receives, processes, transmits or stores any Cardholder Data for or on behalf of Customer, Cisco 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 payment card information, including those established by applicable governmental regulatory agencies, the Payment Card Industry (the "PCI"), all applicable networks, and any written standards provided by Customer's information security group to Cisco from time to time (all the foregoing collectively the "PCI Compliance Standards").

c. Where Cisco Processes Protected Health Information (as that term is defined by The Health Insurance Portability and Accountability Act, or HIPAA), the Business Associate Agreement will be added as Attachment C and will also apply to the Processing of such data. If any of the Applicable Laws are superseded by new or modified mandatory applicable law (including any decisions or interpretations by a relevant court or governmental authority relating thereto), the new or modified mandatory applicable law shall be deemed to be incorporated into this DPE, and Cisco will promptly begin complying with such mandatory applicable law.

d. If this DPE does not specifically address a particular data security or privacy standard or obligation, Cisco will use appropriate, Generally Accepted Practices to protect the confidentiality, security, privacy, integrity, availability, and accuracy of Personal Data.

e. Cisco agrees that, in the event of a breach of this DPE, whether Customer has an adequate remedy in damages, Customer may be entitled to seek injunctive or equitable relief to immediately cease or prevent the use, Processing, or disclosure of Personal Data not contemplated by Cisco's obligations to the Customer and/or this MDPA and to enforce the terms of this DPE or enforce compliance with all mandatory applicable law.

f. Any ambiguity in this DPE shall be resolved to permit Customer to comply with all mandatory applicable law. In the event and to the extent that the mandatory applicable law impose stricter obligations on Cisco than under this DPE, the mandatory applicable law shall prevail.

3. CERTIFICATIONS

a. Cisco must maintain the certifications listed in an applicable agreement between the Parties, if any, and Cisco shall recertify such certifications as reasonably required. If there is a material change in the requirements of a required certification or the nature of the Performance Cisco is providing, such that Cisco no longer wishes to maintain such certifications, the Parties will discuss alternatives and compensating controls in good faith.

b. Prior to Processing Personal Data and at Customer's request, Cisco will provide Customer with copies of any certifications it maintains (along with relevant supporting documentation) that apply to the systems, policies, and procedures that govern the Processing of Personal Data. Cisco will notify Customer if Cisco has failed or no longer intends to adhere to such certifications or successor frameworks. This notification may be provided by posting or publication on Cisco's public website.

4. DATA PROTECTION AND PRIVACY

a. The Parties agree that, for the Personal Data, Customer shall be the Data Controller and Cisco shall be the Data Processor.

b. Customer shall:

i. in its use of the Products and/or Services, comply with mandatory applicable law, including maintaining all relevant regulatory registrations and notifications as required under mandatory applicable law;

ii. ensure all instructions given by it to Cisco in respect of Personal Data shall at all times be in accordance with mandatory applicable law;

iii. have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data, including providing any required notices to, and obtaining any necessary consent from, its employees, agents or third parties to whom it extends the benefits of the Products and/or Services; and

iv. keep the amount of Personal Data provided to Cisco to the minimum necessary for the performance of the Products and/or Services.

c. If Cisco has access to or otherwise Processes Personal Data, then Cisco shall:

i. implement and maintain commercially reasonable and appropriate physical, technical, and organizational security measures described in this DPE (including any appendices or attachments or referenced certifications) designed to protect Personal Data against accidental or unlawful destruction; accidental loss, alteration, unauthorized disclosure or access; all other unlawful forms of Processing; and any Information Security Incident;

ii. take reasonable steps designed to ensure the reliability of its staff and that they are subject to a binding written contractual obligation with Cisco to keep the Personal Data confidential (except where disclosure is required in accordance with mandatory applicable laws, in which case Cisco shall, where practicable and not prohibited by mandatory applicable law, notify Customer of any such requirement before such disclosure) and any other person acting under its supervision who may come into contact with, or otherwise have access to

and Process Personal Data; and require that such personnel are aware of their responsibilities under this DPE and any mandatory applicable law (or Cisco's own written binding policies that are at least as restrictive as this DPE);

iii. appoint data protection lead(s). Upon request, Cisco will provide the contact details of the appointed person;

iv. assist Customer as reasonably needed to respond to requests from supervisory authorities, data subjects, customers, or others to provide information (including details of the Services provided by Cisco) related to Cisco's Processing of Personal Data;

v. not transfer Personal Data from the EEA or Switzerland to a jurisdiction which is not an Approved Jurisdiction, unless it first provides Customer advance notice and an opportunity to object; if Customer reasonably objects to the proposed cross border transfer the applicable Performance that is the subject matter of the objection shall terminate.

Where Cisco Processes Personal Data from the EEA or Switzerland on behalf of Customer, Cisco shall perform such Processing in a manner consistent with the Privacy Shield Principles (see www.commerce.gov/privacyshield) or its successor framework(s) to the extent the Principles are applicable to Cisco's Processing of such data. If Cisco is unable to provide the same level of protection as required by the Principles, Cisco shall promptly notify Customer and cease Processing. In such event, Customer may terminate the applicable Performance of such Processing by written notice within thirty (30) days.

vi. for jurisdictions other than the EEA or Switzerland, not transfer Personal Data outside of the jurisdiction where the Personal Data is obtained unless permitted under mandatory applicable law and it first provides Customer advance notice and an opportunity to object; if Customer reasonably objects to the proposed cross border transfer the applicable Performance that is the subject matter of the objection shall terminate.

Where Cisco Processes Personal Data from an APEC Member Economy on behalf of Customer, Cisco shall perform such Processing in a manner consistent with the APEC Cross Border Privacy Rules Systems requirements ("**CBPRs**") (see www.cbprs.org) to the extent the requirements are applicable to Cisco's Processing of such data. If Cisco is unable to provide the same level of protection as required by the CBPRs, Cisco shall promptly notify Customer and cease Processing. In such event, Customer may terminate the applicable Performance of such Processing by written notice within thirty (30) days.

d. In addition, if Cisco Processes Personal Data in the course of Performance of its obligations to the Customer, then Cisco shall also:

i. only Process the Personal Data in accordance with Customer's documented instructions, Appendix 1 of Attachment C and this DPE, but only to the extent that such instructions are consistent with mandatory applicable laws. If Cisco reasonably believes that Customer's instructions are inconsistent with mandatory applicable law, Cisco will promptly notify Customer of such;

ii. if required by mandatory applicable law, court order, warrant, subpoena, or other legal or judicial process to process Personal Data other than in accordance with Customer's instructions, notify Customer of any such requirement before Processing the Personal Data (unless mandatory applicable law prohibits such information on important grounds of public interest);

iii. only process or use Personal Data on its systems or facilities to the extent necessary to

Perform its obligations solely on behalf of Customer and only for the purposes contemplated by the Parties;

iv. where applicable, act as a subprocessor of such Personal Data;

v. maintain reasonably accurate records of the Processing of any Personal Data received from Customer under the Agreement;

vi. make reasonable efforts to ensure that Personal Data is accurate and up to date at all times while in its custody or under its control, to the extent Cisco has the ability to do so;

vii. not lease, sell, distribute, or otherwise encumber Personal Data unless mutually agreed to by separate signed, written agreement;

viii. provide reasonable cooperation and assistance to Customer in allowing the persons to whom Personal Data relate to have access to their data and to delete or correct such Personal Data if they are demonstrably incorrect (or, if Customer or Customer's customer does not agree that they are incorrect, to have recorded the fact that the relevant person considers the data to be incorrect);

ix. provide such assistance as Customer reasonably requests (either on its own behalf or on behalf of its customers), and Cisco or a Representative is reasonably able to provide, with a view to meeting any applicable filing, approval or similar requirements in relation to mandatory applicable law;

x. promptly notify Customer of any investigation, litigation, arbitrated matter, or other dispute relating to Cisco's information security or privacy practices as it relates to Cisco's Performance of its obligations to Customer;

xi. provide such reasonable information and assistance as Customer reasonably requires (taking into account the nature of Processing and the information available to Cisco) to Customer in ensuring compliance with Customer's obligations under mandatory applicable law with respect to:

A. security of Processing;

B. data protection impact assessments (as such term is defined by mandatory applicable law;

C. prior consultation with a supervisory authority regarding high risk Processing; and

D. notifications to the supervisory authority and/or communications to Data Subjects by Customer in response to any Information Security Incident; and,

xii. on termination of the MDPA for whatever reason, or upon written request at any time during the Term, Cisco shall cease to Process any Personal Data received from Customer, and within a reasonable period will, at the request of Customer: 1) return all Personal Data; or 2) securely and completely destroy or erase (e.g. using a standard such as US Department of Defense 5220.22-M, NIST 800-53, or British HMG InfoSec Standard 5, Enhanced Standard) all Personal Data in its possession or control unless such return or destruction is not feasible or continued retention and Processing is required by mandatory applicable law. At Customer's request, Cisco shall give Customer a certificate signed by one of its senior managers, confirming that it has fully complied with this Clause.

5. STANDARD CONTRACTUAL CLAUSES FOR THE PROCESSING OF PERSONAL DATA

If, and only with Customer's prior consent, Cisco Processes Personal Data from the EEA or Switzerland in a jurisdiction that is not an Approved Jurisdiction, the Parties shall confirm there is a legally approved mechanism in place to allow for the international data transfer.

If Cisco intends to rely on Standard Contractual Clauses (rather than another permissible transfer mechanism), the following additional terms will apply to Cisco and Cisco's subprocessors and/or Affiliates who may be Performing on behalf of Cisco:

a. The Standard Contractual Clauses set forth in Attachment D will apply. If such Standard Contractual Clauses are superseded by new or modified Standard Contractual Clauses, the Parties shall promptly enter into the new or modified Standard Contractual Clauses, as necessary.

b. If Cisco subcontracts any Processing of Personal Data (only as expressly allowed by an applicable agreement between the Parties and mandatory applicable law), Cisco will:

    i. Notify Customer in advance of such Processing and provide Customer an opportunity to object prior to Processing; and

    ii. Require that Cisco's subprocessors have entered into written agreements with Cisco in which the subprocessors agree to abide by terms consistent with the applicable portions of the Standard Contractual Clauses with respect to such Personal Data.

c. If necessary to comply with mandatory applicable law, and where reasonably requested by Customer on behalf of its customers, Cisco shall enter into the Standard Contractual Clauses directly with Customer's customers.

6. SUBPROCESSING

a. Cisco shall have a documented security program and policies that provide (i) guidance to its subprocessors with respect to ensuring the security, confidentiality, integrity, and availability of personal data and systems maintained or processed by Cisco; and (ii) express instructions regarding the steps to take in the event of a compromise or other anomalous event.

b. Cisco shall not subcontract its obligations under this DPE to another person or entity, in whole or in part, without providing Customer with advance notice and an opportunity to object; if Customer reasonably objects to the proposed subcontracting, the applicable Performance that is the subject matter of the objection shall terminate.

c. Cisco will execute a written agreement with such approved subprocessors containing terms at least as protective as this DPE and the applicable Exhibits (provided that Cisco shall not be entitled to permit the subprocessor to further subcontract or otherwise delegate all or any part of the subprocessor's Processing without Cisco's prior notice and opportunity to object) and designating Customer as a third party beneficiary with rights to enforce such terms either by contract or operation of law. Further, if privity of contract is required by mandatory applicable law, Cisco shall procure that any such subprocessors cooperates and enters into any necessary additional agreements directly with Customer.

d. Cisco shall be liable and accountable for the acts or omissions of Representatives to the same extent it is liable and accountable for its own actions or omissions under this DPE.

e. Customer acknowledges and expressly agrees that Cisco's Affiliates may be retained as subprocessors, and (b) Cisco and Cisco's Affiliates respectively may engage third-party subprocessors in the course of Performance. Cisco shall make available to Customer a current list of

subprocessors for the respective Services with the identities of those subprocessors ("Subprocessor List") upon Customer's reasonable request.

7. RIGHTS OF DATA SUBJECTS

a. **Data Subject Requests**. Cisco shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, portability, or deletion of such Data Subject's Personal Data. Unless required by mandatory applicable law, Cisco shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer. In addition Cisco shall provide such information and cooperation and take such action as the Customer reasonably requests in relation to a Data Subject request.

b. **Complaints or Notices related to Personal Data**. In the event Cisco receives any official complaint, notice, or communication that relates to Cisco's Processing of Personal Data or either Party's compliance with mandatory applicable law in connection with Personal Data, to the extent legally permitted, Cisco shall promptly notify Customer and, to the extent applicable, Cisco shall provide Customer with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication. Customer shall be responsible for any reasonable costs arising from Cisco's provision of such assistance.

8. PERMITTED USE AND DISCLOURE

Notwithstanding anything to the contrary in this MDPA, (i) Cisco may disclose Telemetry Data and Support Data to third parties, provided such data has been aggregated and/or appropriately de-identified to reasonably prevent the identification of any individual natural person or legal entity; (ii) Cisco may use Telemetry Data and Support Data for its own business purposes without attribution or compensation to Customer; and (iii) Cisco may use Administrative Data for its own internal business purposes or to fulfill its obligations to Customer under an applicable agreement. Cisco shall not be required to return or destroy Protected Data that constitutes Administrative Data, Telemetry Data or Support Data and shall continue to be permitted to use and disclose such Administrative Data, Telemetry Data, and Support Data as set forth in this Section 8 (Permitted Use and Disclosure) following the termination or expiration of this MDPA.

ATTACHMENT C

Intentionally left blank.

ATTACHMENT D

Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection (These can be located in their original text on the European Commission website here: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm).

For purposes of this Attachment D:

any reference to “data exporter” means Customer, acting as data exporter on behalf of its EEA or Swiss customer(s) where applicable,

and

any reference to “data importer” means Cisco

each a “**party**”; together “**the parties**”.

The parties have agreed on the following Standard Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of

confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data controller is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data controller is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO ATTACHMENT D

THE STANDARD CONTRACTUAL CLAUSES

This Appendix 1 forms part of the Clauses.

Data exporter

The data exporter is Customer, acting as data exporter on behalf of itself or a customer where applicable. Activities relevant to the transfer include the performance of services for Customer and its customer(s).

Data importer

The data importer is Cisco. Activities relevant to the transfer include the performance of services for Customer and customers.

Data subjects

The personal data transferred may concern the following categories of data subjects: Employees, contractors, business partners, representatives and end customers of customers, and other individuals whose personal data is processed by or on behalf of Customer or Customer's customers and delivered as part of the Services.

Categories of data

The personal data transferred may concern the following categories of data:

Personal Data related directly or indirectly to the delivery of services or Performance, including online and offline customer, prospect, partner, and Cisco data, and personal data provided by customers in connection with the resolution of support requests.

Special categories of data

The personal data transferred may concern the following special categories of data:

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union memberships, and data concerning health or sex life, and data relating to offenses, criminal convictions or security measures.

Processing operations

The personal data transferred may be subject to the following basic processing activities, as may be further set forth in contractual agreements entered into from time to time between Customer and customers: (a) customer service activities, such as processing orders, providing technical support and improving offerings, (b) sales and marketing activities as permissible under applicable law, (c) consulting, professional, security, storage, hosting and other services delivered to customers, including services offered by means of the products and solutions described by Cisco, and (d) internal business processes and management, fraud detection and prevention, and compliance with governmental, legislative, and regulatory requirements.

APPENDIX 2 TO ATTACHMENT D

THE STANDARD CONTRACTUAL CLAUSES

Appendix 2 to Attachment D, the Standard Contractual Clauses, is the Information Security Exhibit ("ISE") located at *Attachment A.*

ATTACHMENT E
GLOSSARY OF TERMS

All capitalized terms not defined in this Glossary have the meanings set forth elsewhere in the MDPA.

a. "**Administrative Data**" means data related to employees or representatives of Customer that is collected and used by Cisco in order to administer or manage Cisco's Performance, or the Customer's account, for Cisco's own business purposes. Administrative Data may include Personal Data and information about the contractual commitments between Customer and Cisco, whether collected at the time of the initial registration or thereafter in connection with the delivery, management or Performance. Administrative Data is Protected Data.

b. **"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" mean beneficial ownership of more than fifty percent (50%) of the voting stock, shares, interest or equity in an entity. In the case of any other legal entity, "control" and "controlled" mean the ability to directly or indirectly control the management and/or business of the legal entity.

c. "**APEC**" means the Asia Pacific Economic Cooperation, a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific. See www.apec.org for more information.

d. "**APEC Member Economy**" means the 21 members of APEC: Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong-China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, and Vietnam.

e. "**Approved Jurisdiction**" means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: **http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.**

f. "**Business Associate Agreement**" means the specific terms and conditions that would be added as Attachment C and would apply when Cisco Processes Protected Health Information

g. "**Cardholder Data**" is a category of Sensitive Personal Data and includes a cardholder's name, full account number, expiration date, and the three-digit or four-digit security number printed on the front or back of a payment card. Cardholder Data is Protected Data.

h. "**Confidential Information**" means any confidential information or materials relating to the business, products, customers or employees of the Customer and includes, without limitation, trade secrets, know-how, inventions, techniques, processes, programs, schematics, software source documents, data, customer lists, financial information, pricing, product development, sales and marketing plans or information that Cisco knows or has reason to know is confidential, proprietary or trade secret information obtained by Cisco from the Customer or at the request or direction of the Customer in the course of Performing: (i) that has been marked as confidential; (ii) whose confidential nature has been made known by the Customer to Cisco; or (iii) that due to their character and nature, a reasonable person under like circumstances would treat as confidential.

i. **"Customer Data"** means all data (including text, audio, video, or image files) that is either provided by a customer in connection with the customer's use of products or services, or data developed at the specific request of a customer pursuant to a statement of work or contract. Customer Data does not include Administrative Data, Financing Data, Support Data or Telemetry Data.

j. "**Data Subject**" means the individual to whom Personal Data relates.

k. **"Customer"** means that party making available Protected Data (whether confidential or not) to the other party.

l. "**EEA**" or "**European Economic Area**" means those countries that are members of European Free Trade Association ("**EFTA**"), and the then-current, post-accession member states of the European Union.

m. "**Electronic Protected Health Information**" or "**Electronic PHI**" shall have the meaning given to such term as set forth in the Business Associate Agreement (to be added as Attachment C if applicable).

n. "**Financing Data**" means information related to Customer's financial health that Customer provides to Cisco in connection with the Agreement. Financing Data is Protected Data.

o. **"Generally Accepted Practices**" refer to the levels of accuracy, quality, care, prudence, completeness, timeliness, responsiveness, resource efficiency, productivity, and proactive monitoring of service performance that are at least equal to the then-current accepted industry standards of first-tier providers of the tasks contemplated in Performance of the Agreement.

p. "**Information Security Incident"** means a successful or imminent threat of unauthorized access, use, disclosure, breach, modification, theft, loss, corruption, or destruction of information; interference with information technology operations; or interference with system operations.

q. "**Performance**" means any acts by either Party in the course of completing obligations contemplated under the Agreement, including the performance of services, providing deliverables and work product, access to Personal Data, or providing Software as a Service ("SaaS"), cloud platforms or hosted services. "**Perform**," "**Performs**," and "**Performing**" shall be construed accordingly.

r. "**Personal Data**" means any information that is about, or can be related to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person. Personal Data shall be considered Confidential Information regardless of the source. Personal Data is Protected Data.

s. "**Process**" means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. "**Processes**" and "**Processing**" shall be construed accordingly.

t. **"Product"** means Cisco-branded hardware and software products that are made generally available.

u. "**Protected Data**" means Administrative Data, Confidential Information, Customer Data, Financing Data, Cardholder Data, Support Data, Telemetry Data, and all Personal Data.

v. "**Protected Health Information**" or "**PHI**" shall have the meaning given to such term as set forth in the Business Associate Agreement (to be added as Attachment C if applicable) and is a category of Personal Data. "Protected Health Information" includes "Electronic Protected Health Information" or "ePHI".

w. **"Cisco"** means the Party receiving Protected Data.

x. "**Representatives**" means either Party and its Affiliates' officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.

y. "**Sensitive Personal Data**" or "**Special Categories of Data**" means personal information that requires an extra level of protection and a higher duty of care. These categories are defined by man-

datory applicable law and include: information on medical or health conditions, certain financial information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, precise geolocation over time, or information related to offenses or criminal convictions. Sensitive Personal Data and Special Categories of Data are each a category of Personal Data that are particularly sensitive and pose greater risk. Customer may require additional privacy responsibilities when dealing with such Personal Data, which will be appended to the Agreement or a statement of work, as applicable.

z. **"Service"** means a Cisco-branded service offering described in an applicable service or offer description, statement of work, or purchase order listed selected by Customer.

aa. **"Support Data"** means information that Cisco collects when Customer submits a request for support services or other troubleshooting, including information about hardware, software and other details related to the support incident, such as authentication information, information about the condition of the product, system and registry data about software installations and hardware configurations, and error-tracking files. Support Data is Protected Data.

bb. **"Telemetry Data"** means information generated by instrumentation and logging systems created through the use and operation of the products and/or services. Telemetry Data is Protected Data.