Master Data Protection Agreement

This Master Data Protection Agreement (**"MDPA"**), effective as of the date of the final signature ("**Effective Date**"), forms part of the Agreement (as defined below), entered into by and between [please complete] having its principal place of business at [please complete] ("**Customer**") on behalf of itself and to the extent required under the Data Protection Laws (as defined below), on behalf of its Affiliate(s) (as defined in the Agreement) and Cisco Systems, Inc. (**"Cisco"**) and its Affiliates (as defined below) (each a "**Party**" and together the "**Parties**") and applies where, and to the extent that, Cisco processes Personal Data as a Processor for Customer when providing Products and/or Services (as defined below) under the Agreement.

Unless otherwise specified in this MDPA, the terms of the Agreement shall continue in full force and effect. All capitalized terms not defined in this MDPA shall have the meanings set forth in the Agreement. Any privacy or data protection related clauses or agreement previously entered into by Cisco and Customer, shall be superseded and replaced with this MDPA.

1. Definitions

1.1. "Affiliates" means companies within the Cisco group that may Process Customer Personal Data in order to provide the Products and/or Services. Such Affiliates include Cisco Systems, Inc., Cisco Commerce India Private Limited, Cisco Systems G.K., Cisco Systems Australia PTY Limited, Cisco Systems Canada CO., Cisco International Limited, Cisco Systems (Italy) S.R.L., Cisco Systems International B.V, and ThousandEyes LLC. Unless otherwise explicitly agreed by the Parties, Meraki LLC and AppDynamics LLC., and any legal entity which became part of the Cisco group of companies through an acquisition or merger are not considered Affiliates for the purposes of this MDPA.

1.2. "Agreement" means the written or electronic agreement between Customer and Cisco or the relevant Cisco Affiliate for the provision of the Services and/or Products to Customer.

1.3. "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.

1.4. "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.

1.5. "Approved Jurisdiction" means a member state of the EEA, or other jurisdiction approved as having adequate legal protections for data by the European Commission, currently found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

1.6. "Controller" means an entity that determines the purposes and means of the processing of Personal Data.

1.7. **"**Data Breach**"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

1.8. **"**Data Protection Laws" means all mandatory applicable laws applicable to the Processing of Personal Data under the Agreement.

1.9. "Data Subject" means the individual to whom Personal Data relates.

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

1.11. **"**GDPR**"** means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

1.12. "Personal Data" means any information about, or 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.

1.13. **"**Privacy Data Sheet(s)**"** means the applicable document located on Cisco's Trust Portal that describes the Processing activities in relation to the Service(s) supplied to Customer under the Agreement.

1.14. "Processing" 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 "**Process**" shall be construed accordingly.

1.15. "Processor" means an entity that processes Personal Data on behalf of a Controller.

1.16. "Product" means Cisco or its Affiliates' branded hardware and software that is purchased under the Agreement.

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

1.18. "Special Categories of Personal Data" means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, certain financial information when identified as such by mandatory applicable law, precise geolocation over time and data related to offenses or criminal convictions.

1.19. "Service" means Cisco or its Affiliates' branded service offering that is purchased by Customer under the Agreement.

1.20. "Standard Contractual Clauses" means the agreement set out in Attachment B as approved by the European Commission for the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection.

1.21. "Subprocessor" means another processor engaged by Cisco or its Affiliates to carry out processing activities in respect of the Personal Data on behalf of the Customer.

2. Obligations of the Parties

2.1. The Parties agree that, for this MDPA, Customer shall be the Controller and Cisco shall be the Processor.

2.2. Customer shall:

a. use the Products and/or Services in compliance with Data Protection Laws;

b. ensure all instructions given by it to Cisco in respect of the processing of Personal Data are at all times in accordance with Data Protection Laws;

c. ensure all Personal Data provided to Cisco has been collected in accordance with Data Protection Laws and that Customer has all authorizations and/or consents necessary to provide such Personal Data to Cisco; and

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

2.3. Cisco shall:

a. only Process the Personal Data in accordance with Customer's documented instructions, the applicable Privacy Data Sheet(s), Appendix 1 to the Standard Contractual Clauses and this MDPA, but only to the extent that such instructions are consistent with Data Protection Laws. Cisco will promptly notify Customer if Cisco reasonably believes that Customer's instructions are inconsistent with Data Protection Laws;

b. ensure its applicable Representatives who may Process Personal Data have written contractual obligations in place with Cisco to keep the Personal Data confidential.

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

d. assist Customer as reasonably needed to respond to requests from supervisory authorities, Data Subjects, customers, or others to provide information related to Cisco's Processing of Personal Data;

e. if required by Data Protection Laws, court order, 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 notification on important grounds of public interest);
f. only Process Personal Data on its systems or facilities to the extent necessary to perform its obligations under the Agreement;
g. where applicable, act as a subprocessor of such Personal Data;
h. maintain records of the Processing of any Personal Data received from Customer under the Agreement;
i. not lease, sell, distribute, or otherwise encumber Personal Data unless mutually agreed to by separate signed, written agreement;
j. provide such assistance as Customer reasonably requests (either on its own behalf or on behalf of its customers), and Cisco or a Representative is able to provide, with a view to meeting any applicable filing, approval or similar requirements in relation to Data Protection Laws;
k. provide such information and assistance as Customer reasonably requires (taking into account the nature of Processing and the information available to Cisco) to enable compliance by Customer with its obligations under Data Protection Laws with respect to:
    i. security of Processing;
    ii. data protection impact assessments (as such term is defined by the GDPR);
    iii. prior consultation with a supervisory authority regarding high risk Processing; and
    iv. notifications to the applicable supervisory authority and/or communications to Data Subjects by Customer in response to any Data Breach;
l. on termination of the MDPA for whatever reason, cease to Process and shall delete any Personal Data received from Customer, or without undue delay will, upon written request of the Customer return, or make available for return, all Personal Data in its possession or control and securely delete or permanently render unreadable or inaccessible existing copies of the Personal Data unless such return or destruction is not feasible or continued retention and Processing is required or is permitted by Data Protection Laws and/or mandatory applicable law. At Customer's request, Cisco shall give Customer confirmation in writing that it has fully complied with this Section k.iv or provide a justification as to why deletion is not feasible.

3. Transfers of Personal Data

3.1. Transfers of Personal Data from EEA or Switzerland or the United Kingdom to third countries**.** Where Cisco Processes Personal Data from the EEA or Switzerland or the United Kingdom on behalf of Customer, in a country which is not an Approved Jurisdiction, Cisco shall perform such Processing in accordance with the Standard Contractual Clauses set out in Attachment B to this MDPA and/or in accordance with Articles 44 to 49 of the GDPR.

3.2. Transfers of Personal Data from jurisdictions other than the EEA or Switzerland or the United Kingdom**.** For jurisdictions other than the EEA or Switzerland or the United Kingdom, Cisco shall not transfer Personal Data outside of the jurisdiction where the Personal Data is obtained unless permitted under Data Protection Laws. 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 the Personal 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 Agreement related to such Processing by written notice within 30 days.

4. Subprocessing

4.1. Cisco shall not subcontract its obligations under this MDPA to new Subprocessors, in whole or in part, without providing Customer with notice (for example, by e-mail or in-application messaging) and an opportunity to object. If Customer objects to the proposed subcontracting on reasonable grounds related to the protection of the Personal Data and the Parties cannot resolve the objection, the Customer may terminate the applicable part of the Agreement with respect only to those Products

and/or Services which cannot be provided by Cisco without the use of the objected to Subprocessors by giving written notice to Cisco.

4.2. Where Cisco appoints a Subprocessor, Cisco will execute a written agreement with the Subprocessor(s) containing terms at least as protective as this MDPA.

4.3. Cisco shall be liable for the acts or omissions of Subprocessors to the same extent it is liable for its own actions or omissions under this MDPA.

4.4. For the purposes of Clause 11 of the Standard Contractual Clauses, Customer provides a general consent to Cisco to engage Subprocessors. Such consent is conditional on Cisco's compliance with this Section 4 of the MDPA.

5. Rights of Data Subjects

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, rectification, portability, objection, restriction or erasure of such Data Subject's Personal Data. Unless required by Data Protection Laws, 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. Cisco shall provide such information and cooperation and take such action as the Customer reasonably requests in relation to a Data Subject request.

6. Security

Controls for the Protection of Personal Data**.** Cisco shall implement and maintain appropriate technical and organizational measures designed to protect the Personal Data as set forth in Attachment A. Cisco regularly monitors compliance with these measures.

7. Audit

7.1. Cisco shall make available to the Customer such information as is reasonably necessary to demonstrate Cisco's compliance with the obligations of this MDPA in accordance with Section 4.8.b - Audits and Certifications, of Attachment A of this MDPA.

7.2. Customer acknowledges and agrees that any exercise of its audit rights under Clause 5(f) of the Standard Contractual Clauses will be conducted in accordance with this MDPA.

8. Notification and Communication

8.1. Notification. Cisco shall notify Customer at: [●]@[●].com within 48 hours of confirmation of a Data Breach relating to Customer's Personal Data. Cisco shall provide all such timely information and cooperation as Customer may reasonably require in order for Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Data Protection Law. Cisco shall further take such measures and actions as it considers necessary to remedy or mitigate the effects of the Data Breach and shall keep Customer informed in connection with the Data Breach.

8.2. Information Security Communication. Except as required by mandatory applicable law, Cisco agrees that it will not inform any third party of a Data Breach referencing or identifying the Customer, without Customer's prior written consent. Cisco shall reasonably cooperate with Customer and law enforcement authorities concerning a Data Breach. Cisco shall retain, for an appropriate period of time, all information and data within Cisco's possession or control that is directly related to any Data Breach. If disclosure of the Data Breach referencing or identifying the Customer is required by mandatory applicable law, Cisco will work with Customer regarding the timing, content, and recipients of such disclosure.

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

8.4. Complaints or notices related to Personal Data. If Cisco receives any official complaint, notice, or communication that relates to Cisco's Processing of Personal Data or either Party's compliance with Data Protection Laws 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.

9. General

9.1. Except for any liability which cannot be limited or excluded under mandatory applicable law, the aggregate liability of Cisco for all Data Breaches and any breach of this MDPA (whether for breach of contract, misrepresentations, negligence, strict liability, other torts or otherwise) shall not exceed US$1,000,000.

9.2. Where a Data Breach and/or breach of this MDPA is also a breach of any confidentiality or non-disclosure obligations in the Agreement, the liability cap in Section 9.1 will apply.

9.3. Nothing in this MDPA is intended to limit the Parties' direct liability towards data subjects or applicable supervisory data protection authorities which cannot be limited by mandatory applicable law.

9.4. No one other than a Party to this MDPA, their successors and permitted assignees shall have any right to enforce any of its terms.

9.5. This MDPA will become effective on the Effective Date and remain in force for the term of Agreement.

IN WITNESS WHEREOF, the Parties have caused this MDPA to be executed by their authorized Representative:

Customer	**Cisco**
Authorized Signature	Authorized Signature
Name	Name
Date	Date

Attachment A

Information Security

1. Scope

This Attachment A 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 Personal Data prior to any Processing under the Agreement.

2. General Security Practices

Cisco has implemented and shall maintain appropriate technical and organizational measures designed to protect Personal 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 Attachment A for its personnel, equipment, and facilities at Cisco's locations involved in Cisco's performance of its obligations under the Agreement.

3. General Compliance

3.1. Compliance. Cisco shall document and implement processes to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security or other security requirements. Such processes shall be designed to provide appropriate security to protect Personal 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, which shall be no less strict than the information security requirements set forth in this Attachment A.

3.2. 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.

3.3. Review of information security**.** Cisco's approach to managing information security and its implementation shall be reviewed at planned intervals or when significant changes occur by appropriate internal or external assessors.

3.4. 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.

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

3.6. 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. Threat and vulnerability assessments must be periodically reviewed and prompt remediation actions taken where material weaknesses are found.

3.7. Processing of Special Categories of Personal Data**.** To the extent that Cisco Processes Special Categories of Personal Data and the security measures referred to in this Attachment A are deemed to provide insufficient protection, Customer may request that Cisco implements additional security measures.

4. Technical and Organizational Measures for Security

4.1. Organization of Information Security

a. 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.

b. 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.

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

d. 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 Personal Data.

4.2. Human Resources Security

a. General. Cisco shall ensure that its personnel are subject to confidentiality obligations 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.

b. Training. Cisco personnel with access to Personal 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 Personal Data and training regarding how to effectively respond to security incidents. Training shall be provided before Cisco personnel are granted access to Personal Data or begin providing Services. Training shall be regularly reinforced through refresher training courses, emails, posters, notice boards, and other training and awareness materials.

c. Background Checks. Cisco shall conduct criminal and other relevant background checks for its personnel in compliance with mandatory applicable law and Cisco's policies.

4.3. Personnel Access Controls

a. Access.

i. Limited Use. Cisco will not use any system access information or log-in credentials to gain unauthorized access to Personal Data or Customer's systems, or to exceed the scope of any authorized access.

ii. Authorization. Cisco shall restrict access to Customer's Personal Data and systems at all times solely to those Representatives whose access is necessary to perform the Services or provide the Products.

iii. 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 Personal Data and systems for any Cisco's personnel or its Representatives reasonably suspected of breaching any of the provisions of this Attachment A; and Cisco shall remove access rights of all employees and external party users upon suspension or termination of their employment, or engagement.

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

b. 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 Personal 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.

c. 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 Personal Data and Cisco shall review users' access rights at regular intervals.

iii. For systems that process Personal 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.

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

e. Least Privilege. Cisco shall limit access to Personal Data to that personnel who need access for the purpose of providing the Services and Products and, to the extent technical support is needed, its personnel performing such technical support.

f. Authentication

i. Cisco shall use industry standard practices to identify and authenticate users who attempt to access 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 for user-level accounts and every 90 days for administrator-level accounts.

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.

vii. Cisco shall implement a multi-factor authentication solution to authenticate personnel accessing its information systems.

4.4. Physical and Environmental Security

a. Physical Access to Facilities

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

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

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

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

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

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

d. Clear Desk. Cisco shall have policies requiring a "clean desk/clear screen" designed to prevent inadvertent disclosure of Personal Data.

4.5. Operations Security

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

b. Security and Processing Controls.

i. 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 Personal Data.
ii. 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.

c. Logging and Monitoring. Cisco shall maintain logs of administrator and operator activity and data recovery events related to Personal Data.

4.6. Communications Security and Data Transfer

a. Networks. Cisco shall, at a minimum, use the following controls to secure its networks that access or Process Personal Data:
i. Network traffic shall pass through firewalls, which are monitored at all times. Cisco must implement intrusion detection systems and/or intrusion prevention systems.
ii. Network devices used for administration must utilize industry standard cryptographic controls when Processing Personal Data.
iii. Anti-spoofing filters and controls must be enabled on routers.
iv. Network, application, and server authentication passwords are required to meet minimum complexity guidelines (at least 8 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 for user-level accounts and ever 90 days for administrator-level accounts; or utilize other strong log-in credentials (e.g., biometrics).
v. 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.
vi. Firewalls must be deployed to protect the perimeter of Cisco's networks.

b. Virtual Private Networks ("VPN"). When remote connectivity to the Customer's or Cisco's network is required for Processing of Personal Data:
i. Connections must be encrypted using industry standard cryptography.
ii. Connections shall only be established using VPN servers.
iii. The use of multi-factor authentication is required.

c. 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 Attachment A. Such policies shall be designed to protect transferred information from unauthorized interception, copying, modification, corruption, routing and destruction.

4.7. System Acquisition, Development, and Maintenance

a. Security Requirements. Cisco shall adopt security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.

b. 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.

4.8. Penetration Testing and Vulnerability Scanning & Audit Reports

a. Testing**.** Cisco will perform periodic vulnerability scans and penetration tests on its internet perimeter network. These scans and tests will be conducted by highly qualified professionals, including among other entities, Cisco's compliance team, using industry standard tools and methodologies.

b. Audits and Certifications**.** Cisco shall cooperate with reasonable requests by Customer for legally required security audit (subject to mutual agreement on the time, duration, place, scope and manner of the audit), and respond to reasonable requests for testing reports. Cisco shall make available to Customer, upon written request and without undue delay, copies of any third party audit reports or certifications it maintains (such as SSAE 16 – SOC1, SOC2, SOC3 attestations or ISO 27001:2013 certifications (or their equivalent under any successor standards)) that apply to the Service, to the extent that Cisco maintains such certifications in its normal course of business.

Customer shall treat the contents of reports related to Cisco's security and certifications as confidential information.

c. Remedial Action**.** If any penetration test or vulnerability scan referred to in Section a, 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 considering Cisco's prioritization of such, based upon their criticality (e.g. nature, severity, likelihood).

d. Status of Remedial Action**.** Upon request, Cisco shall keep Customer reasonably informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same.

4.9. Contractor Relationships

a. Policies. Cisco shall have information security policies or procedures for its use of Representatives that impose requirements consistent with this Attachment A.

b. 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.

4.10. Management of Data Breaches and Improvements

a. Responsibilities and Procedures. Cisco shall establish procedures to ensure a quick, effective, and orderly response to Data Breaches.

b. Reporting Data Breaches**.** Cisco shall implement procedures for Data Breaches to be reported as appropriate. All employees and Representatives should be made aware of their responsibility to report Data Breaches as quickly as reasonably possible.

c. 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.

d. 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 a Data Breach. The classification scale should be based on the impact and extent of an incident.

e. Response Process**.** Cisco shall maintain a record of Data Breaches 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.

4.11. Information Security Aspects of Business Continuity Management

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

b. Data Recovery. Where and as applicable, Cisco shall design redundant storage and procedures for recovering data in its possession or control in a manner sufficient to reconstruct Personal Data in its original state as found on the last recorded backup provided by the Customer or in a manner sufficient to resume the Service.

Attachment B

Standard Contractual Clauses (processors)

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 B: 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 To Attachment B.

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.

2. 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.

3. 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.

4. 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).

5. 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.

6. 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.

7. 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.

8. 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).

9. Clause 9 - Governing Law

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

10. 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.

11. 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.

12. 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.

On behalf of the data exporter:
Name (written out in full):
Position:
Address:

Signature……

On behalf of the data importer:
Name (written out in full):
Position:
Address: 170 West Tasman Drive, San Jose, CA 95134, USA

Signature……

Appendix 1 To Attachment B

The Standard Contractual Clauses

This Appendix 1 forms part of the Clauses.

1. 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).

2. Data exporter

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

3. 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.

4. 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 and Products, including online and offline customer, prospect, partner, and Cisco data, and personal data provided by customers in connection with the resolution of support requests.

5. 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.

6. 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 mandatory 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.

DATA EXPORTER	DATA IMPORTER
Name: ……..	Name: ……
Authorised Signature …….	Authorised Signature ……

Appendix 2 To Attachment B

The Standard Contractual Clauses

Appendix 2 to Attachment B, the Standard Contractual Clauses, is the Information Security measures located in Attachment A.