ServiceGrid Smart Bonding for Technical Services (TS)
Offering Description

The ServiceGrid Smart Bonding Description ("**Offering Description**") describes the offerings comprising ServiceGrid Smart Bonding (the "**Offering**") that Cisco Systems and its affiliates ("**Cisco**") or Cisco Approved Sources will provide to the applicable customer or partner ("**Customer**"). The specific quantity and type of Offering will be documented in a written ServiceGrid Smart Bonding Order between the parties or as ordered by Customer via Cisco's website or Support Portal (**"Order"**). The Order may detail the unique requirements agreed between the parties ("**Quote**").

Direct or Indirect Purchases

- **Direct Sale from Cisco.** If a customer ("End User") has purchased this Offering directly from Cisco, this document is incorporated into Cisco Universal Cloud Terms ("**SaaS Agreement**"). If there is a conflict between this Offering Description and the Saas Agreement, this Offering Description shall govern. The terms of this Offering Description are limited to the scope of this Offering Description and Order Form or Statement of Work (SOW) under which the Offerings are ordered and shall not be applicable to any other Offering Descriptions or SOW.
- **Sale through Cisco-Authorized Reseller**. If you are buying through a reseller, you accept the terms of the Saas Agreement by using the Offering, unless the Saas Agreement is otherwise incorporated into your arrangement with the reseller. All non-conflicting and additional terms and conditions in your purchase agreement with reseller remain applicable to this purchase, as between you and your reseller. Your use of the Offering (independent of the purchase terms) is governed by the Saas Agreement and the Saas Agreement takes precedence in regards how you use the Offering. This document is not a contract between you and Cisco. The contract, if any, governing the provision of this Offering is the one between Customer and its Cisco Approved Reseller. Such Cisco Approved Reseller should provide this document to Customer, or Customer can obtain a copy of this and other Cisco Offering Descriptions at www.cisco.com/go/servicedescriptions.

Related Documents. This Offering Description should be read in conjunction with the other applicable documents found at www.cisco.com/legal/services.html

Defined Terms. Capitalized terms are defined in the Glossary of Terms at the end of this document. Capitalized terms used in this Offering Description and not otherwise defined in the Offering Descriptions have the meanings given them in the Agreement.

Cisco reserves the right to change this Offering Description at any time.

1. OVERVIEW

1.1 Summary of Offering

The Offering is an integration software platform in the cloud that seamlessly connects organizations to enable real time multi-party support collaboration for key ITIL-based Workflow processes such as Service Request Management, Incident Management and Change Management.

The Offering:

- provides Customers with tailored capabilities to integrate and automate the end-to-end lifecycle of key Workflow processes used in the delivery of Cisco's Technical Services (TS) offers;
- requires a minimum of one active Business-to-Business Connection (B2B Connection) between the Customer and Cisco for the term of the SaaS subscription, which is normally co-terminus with the service contract of the applicable Cisco TS service offer purchased;
- requires a minimum one year SaaS subscription commitment from the Customer;
- is developed and maintained by Cisco. Its features and functions are continuously enhanced via scheduled product updates normally released quarterly;
- allows Customers to address process integration challenges (i.e. scalability, adaptability) as they evolve their business and require additional process integrations with key business partners;
- is offered as a hosted, public cloud-based solution operated by Cisco from highly secure data center locations;
- includes the Offering's software platform that runs on a high-availability architecture operated around the clock (24x7x365) with a monthly availability target of 99.95% for the Offering's software application as defined in the Platform Availability section in Annex B of this Offering Description; and
- includes standard maintenance and operational support as defined in the Offering Operations section of this Offering Description.

	ServiceGrid Smart Bonding for TS
One active Business-to-Business (B2B) Connection between Customer and Cisco Technical Assistance Center (TAC) using Cisco's standard Transfer Workflow	✓
Standard operational support including break/fix support and monitoring of the B2B Connection with Cisco	✓
Ongoing ServiceGrid Smart Bonding software platform maintenance and feature updates	✓
Additional RMA Workflow added to an existing B2B Connection with Cisco TAC that enables Customers to create, monitor, update and close Return Materials Authorization (RMA) Tickets with Cisco TAC	✓

1.2 Packages and Features

ServiceGrid Smart Bonding for Technical Services (TS):

- ServiceGrid Smart Bonding for TS enables Customers with an active TS service contract to create, monitor, update and close Tickets associated to standard Workflows with Cisco's Technical Assistance Center (TAC) in the normal day-to-day delivery of Cisco Technical Services offers.
- This Offering includes:
  - one B2B Connection between Customer's IT Service Management (ITSM) application and Cisco's ITSM application utilizing Cisco's standard Transfer Workflow;
    - Transfer Workflow enables Customers, as well as Cisco, to work out of the convenience of their own ITSM applications to create, monitor, update and close Tickets in the normal delivery of Cisco TS offers;
  - standard operational support including:
    - break/fix support and monitoring of the B2B Connection with Cisco;
    - ongoing ServiceGrid Smart Bonding software platform maintenance and feature updates;
    - if desired, access to ServiceGrid portal for Customer to communicate system maintenance windows (downtime) to Cisco and self-maintain authentication certificates;
- Optional Offering elements include:
  - additional RMA Workflow that enables Customers, as well as Cisco, to work out of the convenience of their own ITSM applications to create, monitor, update and close Tickets specifically associated to Return Materials Authorization (RMA) service requests with Cisco;
    - An active B2B Connection with Transfer Workflow is a pre-requisite for enabling additional RMA Workflow. Separate purchase of Cisco Advanced Services will be required to implement the RMA Workflow.

2. OFFERING ACTIVATION

2.1 Overview and Timeline

After Cisco receives a signed Customer purchase order for the Offering and enters the order in Cisco's ordering system, Cisco will perform the following Initial Fulfilment Activities to enable the Customer to utilize the features and functions of the Offering.

Cisco responsibilities include:

- Analyzing, implementing, testing and activating Customer's B2B Connection with Cisco (additional Advanced Services purchase required); and
- Notifying Customer of completion of these activities.

The Offering term will commence when the Initial Fulfilment Activities have been completed. Initial Fulfilment Activities are normally completed within 90-days from the entry of Customer's order in Cisco's ordering system. Cisco will make all reasonable commercial efforts to complete Initial Fulfilment Activities within this 90-day window and requires Customer to work closely with Cisco and commit all necessary resources to complete Initial Fulfilment Activities.

2.2 Customer Requirements

- *Compliance Review.* Cisco will have the right, upon reasonable notice, to audit Customer's records during normal business hours to ensure Customer's compliance with all terms and conditions of the Offering. Cisco will bear the cost of the audit unless it is found that Customer is misusing the Service.

- *Data Backup.* Maintain appropriate protection and backup of End User data and content residing on Customer controlled systems and applications at all times. Customer assumes full responsibility to back-up and/or otherwise protect all data against loss, damage, or destruction. Customer acknowledges that it has been advised to back-up and/or otherwise protect all data against loss, damage or destruction.

- *Environment.*
  - Not tamper with or interfere with any Cisco provided infrastructure or software, but may use the features of the Offering, as provided or referenced in the Offering Description or associated Documentation. This includes, but is not limited to, server, storage, networking, racking, HVAC, cabling, power, network connectivity, as well as, software and hardware updates or upgrades to any infrastructure not directly controlled by Cisco.
  - Customer must notify Cisco of any change to its system requirements in a timely manner before the commencement of Cisco Offering and Customer is responsible for any delay and additional costs, which arise due to any change in its system requirements.

- *Information and Reasonable Assistance*.
  - Customer shall supply Cisco with all reasonably requested and reasonably necessary, accurate, complete, and up to date information and assets to allow Cisco to supply the Offering to the Customer. Provide updated and accurate information on Customer's hardware and software environment, networking information, and similar information reasonably required or requested to provide the Offering. Customer will reasonably work with Cisco in a timely manner to aid in Cisco's provision of the Offering to Customer by any third party cooperation, documents or approvals required for provision of Cisco's Offering.
  - Customer shall provide all necessary support in connection with the implementation and operation of Offering, including granting Cisco employees access to necessary premises during regular business hours as may be required for the performance of the Offering and granting adequate access to the Customer's production and testing (staging) systems (hardware and software), and ensuring the cooperation of the Customer's employees as required. If any cooperation or document is not provided as requested, the delivery and performance dates will be postponed at least by the period caused by the delay and the Customer shall reimburse Cisco for any wasted or additional expenses caused thereby.

- *Issue Triage & Resolution***.** Provide technical resources to capture and provide details of reported issues, to aid in replication and triaging issues as reasonably requested by Cisco, to aid in testing fixes of issues, to confirm issues are not related to End User provided hardware, software, applications, or other sources.

- *Secure Adoption*
  - Customer must not use the Offering to send spam, viruses or malware.
  - Customer is responsible for any catastrophic security events that result from any unauthorized configuration of the Offering components by Customer's personnel. These include, but are not limited to, configuring the Offering components in a manner not prescribed in the Documentation, creating an open relay, changing the network configuration set by Cisco, shutting down Cisco's infrastructure, etc.
  - Customer may be assigned a user ID and a password for the use of the Offering and Customer shall protect the access authorization against third-party access and shall immediately modify the same if a third party may have become aware thereof. Customer shall ensure the access authorization may be used only by that to whom it was assigned. Cisco shall not be liable if a third party uses or abuses Cisco Offering with a user ID assigned to the Customer. The Customer shall indemnify and hold Cisco harmless in respect of any damage Cisco may incur as a result from such use or abuse.

3. OFFERING OPERATIONS

3.1 Support and Escalation Guidelines

- Cisco operates a 24/7 helpdesk. If engineers are unable to resolve the issue they will escalate the issue internally for resolution.
- Customer is responsible for using reasonable efforts to resolve internally any support questions prior to contacting Cisco. Customer is responsible for reporting any and all errors promptly in writing in English and for providing sufficient information to Cisco to enable Cisco to duplicate the circumstances indicating a reported Software defect or error. Customer shall provide technical information as may be required by Cisco systems engineers or security analysts, including but not limited to IP addresses for Customer's existing solution.
- A TAC Service Request can be opened in multiple ways via:
  1) *Service Request Tool.* The online Service Request Tool via "Cisco.com" allows Customer to enter information pertaining to the issue.
  2) *Email*. Customer can send an email to tac@cisco.com including the problem description and contact details; or

3) *Phone***.** Customer can use the phone. When Customer calls Cisco's Technical Support number the call gets transferred to a Customer Interaction Network (CIN) Agent who captures the initial information about Customer's Service Request and routes the call to the appropriate engineering resource. The CIN team handles all incoming telephone and e-mail messages. The CIN agent completes the following functions for each Service Request: a) open a case, b) verify Customer's entitlement, c) discuss and set priority (Customer sets the severity 1-4) and d) dispatch to the appropriate TAC team.

Help Desk

Telephone	Email	Web
Cisco Worldwide Support Contacts	tac@cisco.com	https://mycase.cloudapps.cisco.com/case

Severity Definitions
Cisco help desks shall assign a severity to all problems submitted by Customer

- ***"Critical Event" or "Severity 1".*** Cisco ServiceGrid environment or application is down or there is a critical impact to Customer's business operations. The Customer and Cisco will commit full-time resources to resolve the situation.

- ***"Major Event" or "Severity 2".*** Operation of an existing environment or application is severely degraded or significant aspects of the Customer's business operations are negatively impacted by unacceptable environment or application performance. The Customer and Cisco will commit full-time resources during Standard Business Hours to resolve the situation.

- ***"Minor Event" or "Severity 3".*** Operational performance of the environment or application is impaired, although most business operations remain functional. The Customer and Cisco are both willing to commit resources during Standard Business Hours to restore service to satisfactory levels*.*

- ***"Information Request"*** *or* ***"Severity 4".*** Information or assistance is required on product capabilities, installation, or configuration. There is clearly little or no impact to Customer's business operation. Cisco and Customer are both willing to provide resources during Standard Business Hours to provide information or assistance as requested.

Escalation process
- Customer should engage the below contacts when an issue requires escalation.
- Severity 1 escalation times are measured in calendar hours – 24 hours per day, 7 days per week. Severity 2, 3, and 4 escalation times correspond with Standard Business Hours.
- Inquiries can be made via email and are answered by qualified Cisco ServiceGrid Customer Support Engineers during standard business hours (08:00-22:00 UTC).
- All inquiries will be prioritized based on the determined level of severity as described above in the severity definitions.
- Cisco recommends that Customers call the Cisco TAC support hotline if they detect (or perceive) a Severity 1 type of issue as described above.
- Service Level Objective (SLO) for Time-to-Respond (TTR) is:
    - 1 hour or less for Severity 1 and Severity 2 cases; and
    - Next Business Day (NBD) for Severity 3 and Severity 4 cases.

Elapsed Time	Severity 1	Severity 2	Severity 3	Severity 4
1 hour	Senior Customer Service Technician			
4 hours	Service Level Manager	Senior Customer Service Technician		
24 hours	Technical Support Manager	Service Level Manager		
48 hours	Director, Technical Support	Technical Support Manager		
72 hours		Director, Technical Support	Service Level Manager	
96 hours			Technical Support Manager	Service Level Manager

3.2 Maintenance and Updates

- From time to time, Cisco performs scheduled maintenance, to update the servers and software that are used to provide the Offering. Cisco will make all reasonable attempts to notify Customer at least two business days in advance of any planned downtime or scheduled maintenance. Notwithstanding the foregoing, Customer

acknowledges that Cisco may, in certain situations need to perform emergency maintenance without providing advance notice.

- Cisco reserves the right to modify and update the features and functionality of the Offering, at no additional cost to Customer, with the objective of providing Customer with equal or enhanced Offering. These updates shall include any subsequent release or version of the Offering containing functional enhancements, extensions, error corrections or fixes which are generally made available free of charge to customers who have contracted for the appropriate level of Offering. Updates shall not include any release, option or future product which Cisco licenses separately or which is not included under the applicable level of support.

- Cisco provides ongoing software releases and updates as a standard part of the Offering. Cisco will give Customer prior written notice of any material modification or update. Cisco will use reasonable efforts to ensure that any modifications or updates do not materially degrade the performance of the Offering or Customer's use thereof. Cisco will ensure that any modifications or updates do not require Customer to incur any material additional cost to continue its use of the Offering.

- Cisco will use reasonable efforts to implement modifications or updates in a manner that minimizes the impact on Customer's use of the Offering. Cisco will normally give Customer advanced notice of planned maintenance. Cisco may need to carry out emergency maintenance at any time in the event of an emergency (without prejudice to Service Level Objectives as provided in Annex B).

3.3 Connection Monitoring

The Offering's software platform is actively monitored by Cisco (24x7x365). Operational disturbances are automatically detected and Cisco support engineers are immediately notified.
An operational disturbance is generally defined as:

- A failure of the Offering platform;
- The non-availability of Customer's interface (e.g. messages cannot be sent from Cisco to Customer); or
- The non-availability of Cisco's interface (e.g. messages cannot be sent from Customer to Cisco).

Cisco cannot auto-detect every problem at Customer side (e.g. messages cannot be sent to the Offering's software platform). When Cisco does detect operational disturbances, an email notification is sent to Customer for all outage-related incidents unless Customer has negotiated additional service level terms with Cisco.

ANNEX A
Glossary of Terms

B2B Connection is a business-to-business connection between Customer and Cisco via the Cisco ServiceGrid integration platform. Customer's ITSM application is logically connected to the Cisco ServiceGrid platform to enable the automation of a service Workflow that includes data, attachments and status exchange transactions.
Cisco ServiceGrid is an integration platform in the cloud that seamlessly connects Customers to enable real time multi-party support collaboration for key ITIL-based Workflow processes including, but not limited to, Service Request Management, Incident Management and Change Management.
Data Terms governs the manner in which each of Cisco and Customer will protect any User Data as described in the Data Privacy section of Annex B in this Offering description.
Information Technology Service Management (ITSM) applications enable Customers to execute and manage service related Tickets internally. Cisco ServiceGrid enables Customers to integrate and automate Workflow processes with Cisco by creating B2B Connections between Customer's ITSM application and the ITSM applications used within various Cisco services practices.
Initial Fulfilment Activities are a set of activities that Cisco will complete to activate the ServiceGrid Smart Bonding Offering for the Customer. These activities include analyzing, implementing, testing and activating a live B2B Connection between Customer and Cisco and notifying Customer of the completion of these activities.
Tickets are generally defined as service requests, incidents, and change requests associated to Workflow processes between Customer and Cisco. Tickets can also be referred to as support cases, service cases, service requests, incidents and change requests.
User Data includes names, job titles, contact information or other sensitive information related to users of the Offering.
Workflows - Tickets are driven through a pre-defined set of Workflow tasks and transactions triggered through a series of updates made by Customer or Cisco. Each update and its data are stored in Cisco ServiceGrid database. Workflows are the basic method to manage Tickets with Cisco.

- Standard Workflows applicable to Cisco Technical Services (TS) include:

  - **Transfer Worflow** which enables Customer, as well as Cisco, to work out of the convenience of their own ITSM applications to create, monitor, update and close Tickets with Cisco during normal day-to-day delivery of Cisco TS offers; and
  - **RMA Workflow** which enables Customer, as well as Cisco, to work out of the convenience of their own ITSM applications to create, monitor, update and close Return Materials Authorization (RMA) Tickets with Cisco during normal day-to-day delivery of Cisco TS offers.
- Standard Workflows applicable to Cisco Cloud and Managed Services (CMS) include:
  - **Service Request Management Workflow** which enables Customer, as well as Cisco, to work out of the convenience of their own ITSM applications to create, monitor, update and close Service Request Tickets during the normal day-to-day delivery of Cisco CMS offers;
  - **Incident Management Workflow** which enables Customer, as well as Cisco, to work out of the convenience of their own ITSM applications to create, monitor, update and close Incident Tickets during normal day-to-day delivery of Cisco CMS offers; and
  - **Change Management Workflow** which enables Customer, as well as Cisco, to work out of the convenience of their own ITSM applications to create, monitor, update and close Change Tickets during normal day-to-day delivery of Cisco CMS offers.

ANNEX B
Additional Terms for SaaS Offerings

1. Commercial Terms

Invoicing. Once Cisco has received and accepted the Purchase Order and entered the Customer's order in Cisco's ordering system, Cisco will complete the Initial Fulfillment Activities to activate the Offering for the Customer. Once these Initial Fulfillment Activities are completed the start date for the Offering's subscription term will begin. This start date will trigger invoicing for all SaaS subscription elements included on the Purchase Order.

Initial Fulfilment Activities are completed within 90-days from the entry of the Customer's order in Cisco's ordering system. Cisco will make all reasonable commercial efforts to complete Initial Fulfilment Activities within this 90-day window and subsequently requires Customer to commit all necessary resources to complete Initial Fulfilment Activities. If Customer is responsible for delays which extend Initial Fulfilment Activities beyond the normal 90-day window Cisco will begin the Offering subscription start date 90 days past the Cisco order entry date and invoice the Customer accordingly per the terms of the Offering.

The invoicing schedule will be based on the Customer's preferred invoicing terms, as selected, for the term of the Offering subscription. Available invoicing options include: 100% upfront pre-paid; monthly in advance; quarterly in advance; or annual invoicing in advance. Annual invoicing is the default if no invoicing preference is selected at the time the order is processed. All invoices are net 30 payment terms.

Subscription Termination. Upon termination of the Offering subscription, Cisco will de-provision the Customer from the Offering's software platform and disconnect all Customer systems and user access (if applicable). This de-provisioning and deactivation may include any/all software related to the Offering residing on the Offering's platforms.

2. Platform Availability

Cisco provides the Offering's software integration platform via SaaS with the defined service deliverables as described in this Offering Description.

The data, programs and applications are run on high-availability cluster systems. The Service Level Objective (SLO) availability target of the software application of the Offering is 99.95%, which is measured on a 24x7x365 basis. Interruptions caused by the infrastructure of the Customer do not count against the Offering software application availability service level. Availability is measured by regular requests of online services and B2B connection interfaces from several locations worldwide.

The Offering software platform is regularly updated. This is done through new application releases (normally on a quarterly basis). Releases are normally set into operation during scheduled maintenance windows (see Maintenance and Updates section).

Maintenance windows are announced in advance and are normally planned and executed afterhours on a weekend. Maintenance windows do not count against the availability service level.

New releases are announced in advance and release notes are published along with each new release. For more details see Maintenance and Updates section in this document.

The availability and performance of the Offering's software platform is permanently monitored and measured by Cisco. Platform availability metrics are available upon request.

3. Data Privacy and Security

Security. The scope of the Offering Security Policy includes:

- Defense of the hosted application and data against external attacks;
- Availability of functions and data;
- Secure communication of data between Customers, their Ecosystem Trading Partners, and Cisco;
- Access through Web functions and multi-tenant architecture; and
- Clear permission / role-based access policy.

Although Cisco does not warrant that the Offering's software application and its data will be free of vulnerability to intrusion or attack, Cisco does follow appropriate security practices to protect the Offering software application and its data against external attacks and to avoid intrusion by segmentation into different network zones that are segregated by rigorous firewall policies.

The connection to Offering is by means of encrypted connections and requires authentication. The table below describes the transport method, authentication and encryption method utilized.

Transport Method	**Authentication**	**Encryption**
Transaction-based via HTTPS POST	Authentication via Login and Password	HTTPS (SSL)
Transaction-based via HTTPS SOAP	Authentication via Login and Password	HTTPS (SSL)
Transaction-based via REST over HTTPS	Authentication via Login, Password and OAUTH2	HTTPS (SSL)

Data Privacy. In using the Offering, Customers will transmit Service Cases, which Service Cases may include users' names, job titles and contact information, as well as other information that may be considered sensitive (any such names, job titles, contact information or other sensitive information, "User Data"). This section (these "Data Terms") governs the manner in which each of Cisco and Customer will protect any User Data. Customer's right to use the Offering is conditioned on Customer's adherence to these Data Terms. In the event of a conflict between your Agreement, Cisco's Privacy Policy and/or these Data Terms, the following order of precedence applies to the subject matter of this Offering Description: (a) the Agreement, (b) these Data Terms, and (c) Cisco's Privacy Policy.

The Offering will collect User Data only in the course of use of the Offering and will not collect any information when a User is not using the Offering. Unless otherwise agreed by the parties in writing, User Data will be hosted by Cisco and/or its authorized subcontractors.

For purposes of these Data Terms, "Privacy Laws" are defined as all applicable laws and regulations relating to privacy or the collection, use, storage and other forms of and processing of personal or consumer data, including where applicable guidance and codes of practice issued by any relevant supervisory authority.

Customer responsibilities:
a) Customer has and will maintain a privacy policy that (i) is available via a link on the landing page of the Customer's website, and (ii) describes the collection and use of User Data generally, including as part of the Offering.
b) Customer will, prior to the submission of User Data to Cisco, obtain consents from every User as may be required and in such form as necessary to comply with applicable Privacy Laws.
c) Customer will not use the Offering to collect information from children under the age of 13 and will not use the Offering to create information requests targeted at children under the age of 13.
d) In the countries and territories in which Customer will use the Offering, Customer will comply with all applicable Privacy Laws. Customer acknowledges that Cisco is accessing and processing User Data at Customer's direction and on Customer's behalf.
e) Other than as necessary to provide the Offering, Customer will not use the Offering for sharing of User Data with third parties without a User's Consent.
Upon Cisco's request, Customer will confirm compliance with these requirements by providing Cisco with a copy of its privacy policy and with access to the user screens that Customer uses to notify users of its privacy practices and to obtain any consents to the collection and use of personal data.

Cisco responsibilities:
a) Cisco will process User Data in accordance with the agreement, with Cisco's Privacy Policy, and in compliance with applicable law.

b) Cisco will not use, disclose or otherwise process User Data other than (i) as reasonably necessary to provide the Offering, (ii) where instructed or permitted by Customer, (iii) to exercise or protect Cisco's legal rights, or (iv) as required by applicable law.
c) Cisco will process User Data in compliance with all Privacy Laws that are directly applicable to Cisco.
d) If Cisco uses a subcontractor for the provision of the Offering, such subcontractor will only process User Data subject to a written agreement that complies with applicable Privacy Laws with respect to Cisco's use of subcontractors for the processing of User Data.
e) Cisco shall maintain procedures to detect and respond to an unauthorized acquisition of or a security breach ("Data Security Incident") affecting unencrypted User Data while such User Data is in its possession or control. Cisco shall promptly notify the Customer of a Data Security Incident as soon as reasonably practicable after Cisco has become aware of it and taken necessary and appropriate steps to contain and determine the extent of the Data Security Incident. Cisco agrees to provide reasonable assistance to assist the Customer in further investigating any such incident, or in providing notice as required by applicable law.
Upon request by Customer in writing, Cisco will assist Customer (i) in complying with any User's exercise of rights under Privacy Laws with respect to User Data processed by Cisco as part of this Offering and (ii) in complying with any inquiry, notice or investigation of Customer's compliance with Privacy Laws, provided that Customer will reimburse Cisco for all reasonable costs arising from any such assistance with compliance.

Customer consents to Cisco using, disclosing or otherwise processing User Data:
a) as reasonably necessary to provide the Offering (including sharing User Data with Customer's B2B Connections),
b) to provide, maintain, and improve the Offering,
c) to exercise or protect Cisco's legal rights,
d) as permitted or instructed by Customer, and
e) as required by applicable law.
Customer also consents to Cisco's use of User Data on an aggregated basis for analytics purposes and to Cisco's disclosure of the results of any such analysis ("Learned Data"), provided that User Data associated with specific Users is not disclosed as the Learned Data.

Customer acknowledges that Cisco is permitted to comply with all applicable laws to which it is subject, as determined in its sole discretion.

Customer will indemnify, hold harmless and defend Cisco, its affiliates, directors, employees and agents from and against, and reimburse Cisco and each of such parties with respect to, any losses, damages, claims, liabilities, costs and expenses (including reasonable attorneys' fees and expenses) related to or arising out of (i) an actual or alleged violation by Customer of Privacy Laws or Customer's own privacy policies, (ii) an investigation by a government agency (such a consumer protection agency, industry regulator or data protection authority) into Customer's use of the Offering, (iii) breach of any duty owed by Customer to its Users, or (iv) any breach of any representation, warranty, covenant or agreement of Customer contained in or made pursuant to this Agreement.

Additional Terms applicable to transactions with Customer if Customer is in one of the Data Protection Countries only, where "Data Protection Countries" means the European Union member states, Norway, Iceland, Liechtenstein, Switzerland and other countries and territories that have adopted legislation substantially similar to EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data:

- Customer acknowledges that Cisco will use the Offering to process User Data as a "data processor" for Customer as such term is used in the data protection legislation of the European Economic Area member states and, where applicable, equivalent legislation in other countries and territories ((or as a subprocessor where Customer acts as a processor of its own end user's data). Customer will be a "data controller" under the applicable data protection laws in relation to all data made available by it.
- Customer consents to the transfer of User Data to Cisco and its subsidiaries in the United States provided that Cisco maintains its certification of compliance with Privacy Laws applicable to Customer with respect to transfers of personal data to countries that have not been deemed to have adequate protections for personal data.
- If Cisco uses a subcontractor for the provision of the Offering, such subcontractor will only process User Data as Cisco's subprocessor.
- With regard to any Data Security Incident, Customer, as the data controller, shall determine whether and when to notify any individuals or persons (including governmental authorities) regarding such Data Security Incident affecting User Data. Notwithstanding the foregoing, Cisco is permitted to comply with all applicable laws to which it is subject, as determined in its sole discretion.

Cisco acknowledges that the Customer may be subject to laws or regulations applicable to the Customer's business relating to data privacy, information security and export control (such as Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, Health Information Technology for Economic and Clinical Health (HITECH) Act, Fair Credit Reporting Act, or Office of Controller of Currency guidelines) (hereinafter "Customer Regulations"). The parties do not expect that Cisco will use or have access to the types of information covered under the Customer Regulations in a way that would require Cisco to become subject to Customer Regulations. While Cisco may not itself be subject to Customer Regulations, Cisco will, upon request, provide the Customer with commercially reasonable assistance and information necessary to enable the Customer to comply with the Customer's own obligations under any applicable

Customer Regulations. The parties acknowledge that Cisco is not agreeing to become subject to any Customer Regulations as a result of this Offering Description (except where such regulations already apply to Cisco as a result of Cisco's own business).

4. Operational Support

Customer must notify Cisco of any change to its system requirements in a timely manner before the commencement of the Offering and Customer is responsible for any delay and additional costs, which arise due to any change in its system requirements.

The following are operational support limitations to the Offering in all theaters:

- Standard support for the Offering is only provided when an active subscription is in place. Any special support arrangements that fall outside of the standard support terms as described in this Offering Description will be specific to Customer's purchase contract and must be negotiated independently upon purchase of the Offering.
- Cisco has no obligation to continue to provide operational support if the Offering's software platform was not used as specified by Cisco specifications and Cisco reasonably believes that such use caused the error or another cause, within the Customer's control, caused the error or a defect in the Offering's software platform.
- Local language support: Designated Cisco personnel will be proficient in English and German and will deliver the Offering in either language per Customer needs. Any other language support will be handled in a custom (statement of work) arrangement, if needed.

Onsite Customer visits: the Offering is delivered via remote Cisco support personnel and does not include any onsite Customer visits by these designated remote resources.