Service Description: Cisco Mobility IQ Term Subscription Service and Data Protection Annex

This document describes Cisco Mobility IQ Services sold by Cisco Systems, Inc. and Cisco Authorized Resellers.

Related Documents: The following documents posted at www.cisco.com/go/servicedescriptions/ should be read in conjunction with this Service Description and are incorporated into this Service Description by this reference: (1) Glossary of Terms (to the extent those terms are not otherwise defined in this Service Description or the agreement under which You purchase services), and (2) List of Services Not Covered.

Direct Sale from Cisco. If You have purchased these Services directly from Cisco Systems, Inc. ("Cisco"), this document is incorporated into Your Master Services Agreement or equivalent services agreement ("MSA") executed between You and Cisco. In the event of a conflict between the MSA and this Service Description, this Service Description shall prevail.

Sales via Authorized Reseller. If You have purchased these Services through a Cisco Authorized Reseller, this document is for informational purposes only; it is not a contract between You and Cisco. The contract, if any, governing the provision of this Service is the one between You and Your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to You, or You can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

Capitalized terms herein shall have the same meaning afforded under the above links, unless otherwise specified herein. The provision of Services by Cisco Mobility IQ assumes that Subscriber will comply with the terms herein.

For ease of reference, whichever agreement under which You are purchasing the Services will be referred to in this Service Description as the "purchase agreement."

Cisco shall provide selected Cisco Mobility IQ Services described below for which Cisco has been paid, and continues to be paid, the appropriate fee.

Cisco Mobility IQ Subscription Services

The Cisco Mobility IQ Subscription Services are offered as:

- Network IQ
- User IQ
- Business IQ

Cisco Mobility IQ Services are not available in all countries. Purchases may be limited or restricted in some markets. If the Service is ordered but is limited or restricted in the end-customer's market, Cisco Mobility IQ will not be able to provision the Service. Contact Your sales representative for further information.

Service Support

Cisco Mobility IQ provides technical support during Standard Office Hours (Pacific Time Zone) Mon-Fri, 06:00-18:00 PST in English to our customers and their attendees. We can be contacted via email at support-miq@cisco.com. Support is available for the duration of Your Subscription.

Cisco Mobility IQ Subscription Details

Mobility IQ is the subscription business model under which You are purchasing the Cisco Mobility IQ Service. Mobility IQ gives the flexibility of bringing APs (up to the purchased quantity) in and out of service without having to provision de-provision specific APs on the service.

Commercial Terms

- A Subscriber is the company purchasing the Cisco Mobility IQ Services, either directly or through a Cisco Authorized Reseller. You are the "Subscriber."
- As a Subscriber, You are buying Active APs. Active APs are APs added to Cisco Mobility IQ portal and seen on the network for 16 or more days in a month. Should the Ordered Quanity of Active APs be less than the actual quantity of active APs the Subscriber will be notified of the overage. Subsequent, consecutive overages in excess of 1% of the subscribed quantity will result in a) the Subscriber needing to place an additional order for the increased amount or b) Cisco will invoice the customer for the average overage. A Subscriber with 3 consecutive overages will be found in violation of this contract and Cisco reserves the right to terminate service.
- While Active APs aren't tied to a specific AP, APs must be added to Cisco Mobility IQ portal to take full advantage of the service. The List of APs will be created and maintained by the Subscriber.

Subscription Quantity

Under the Active APs Subscription model, You do not have to pay for each AP owned but rather only for APs for which You wish to utilize Mobility IQ Services.

Add-On and Upgrades to Cisco Mobility IQ Subscription

Additional features and upgrades are enabled upon request and co-terminus with existing Mobility IQ Services. These "Additional Features" and "Upgrades" are only available with the purchase of Mobility IQ Services and not available on a stand-alone basis. Some Additional Features and Upgrades may be billed on a per use basis. Others are available as a Subscription.

Because Additional Features must be co-terminus with the other Mobility IQ Service, that is, Additional Features may not be purchased on their own the termination date of the Mobility IQ Service will constitute termination of any Additional Feature/Upgrade subscription or use, as applicable, irrespective of any remaining time on the Additional Feature or Upgrade Subscription.

Mobility IQ Cloud Connection

Cloud Connection Implementation Period

To provide a Service Provider quality service, with simple ease of use and because no network is the same, Mobility IQ Services are cloud based and do require integration and implementation Period ("Implementation Period"). Mobility IQ does require provisioning/configuration of few additional components, including an IPSEC tunnel between the Subscribers and Cisco Mobility IQ data centers. Cisco will provide the customer necessary information and configurations within 14 days of order. While, Cisco Support is included and White Glove services are available through Cisco Advanced Services, this implementation is the sole responsibility of the Subscriber. During the Implementation Period, the initial Subscription Term for Mobility IQ Services will not accrue for that period of time in which the Implementation Period is in effect or 60 days whichever is the lessor.

The Implementation Period shall end at Cisco's discretion, at any time, and without further or additional notice. Upon expiration of the Implementation Period, the Subscription Term will begin.

Mobility IQ Included Support

This section describes Cisco Mobility IQ Subscription Support that are included with Mobility IQ Service Subscriptions. These Services are not available for separate purchase.

Direct Sale from Cisco. If You have purchased Software Term Subscription Products that include these Services directly from Cisco, this document is incorporated into Your applicable master purchase agreement with Cisco. In the event of a conflict between this Service Description and Your applicable master purchase agreement, this Service Description shall govern.

Sale via Cisco-Authorized Reseller. If You have purchased these Services through a Cisco-Authorized Reseller, this document is for description purposes only; is not a contract between You and Cisco. The contract, if any, governing the provision of this Service will be the one between You and Your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to You, or You can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

Cisco Responsibilities:

- Cisco Mobility IQ Services Support is available during Standard Office Hours (Pacific Time Zone) Mon-Fri, 06:00-18:00 PST in English to assist by electronic mail or the internet with Mobility IQ Subscriptions use, configuration and troubleshooting issues.
- Access to Cisco.com. This system provides Customer with helpful technical and general information on Cisco Products as well as access to Cisco's on-line Software Center library. Please note that access restrictions identified by Cisco from time to time may apply.
- Work-around solutions or patches to reported Mobility IQ Subscription problems will be provided using reasonable commercial efforts. An advantage of the Mobility IQ cloud based solution is any patches or Maintenance Releases/updates for Mobility IQ users experiencing the problem in their subscription, will be implemented automatically with little or no action on the Subscriber's part.
- Minor and Maintenance Releases/Updates**.** All paying Subscribers will receive updates corresponding to the Mobility IQ service to which they subscribe. Such Updates are limited to Mobility IQ Services that have been validly licensed and paid for and that are covered under a current Term Subscription contract and whose account is in good standing order. Cisco may also release additional features or complementary services that are not included in the subscription and are available at an additional charge. Cisco may from time to time discontinue or remove some features that are deemed as depreciated or have low customer adoption. Applicable supporting Documentation for the latest production version, if available, is on Cisco.com and is limited to only the current production instance of Mobility IQ.

Subscriber Responsibilities:

The provision of the Support options assumes that Customer will:

- Provide a severity level as described in the Cisco Severity and Escalation Guideline (http://www.cisco.com/web/about/doing_business/legal/service_descriptions/docs/Cisco_Severity_and_Escalation_Guidelines.pdf) for all interactions the Subscriber has with Cisco Mobility IQ Support.
- Grant Cisco reasonable access to the Product and Data and systems passwords so that problems may be diagnosed and, where possible, corrected remotely.
- Provide thirty (30) days Notice to Cisco of any requested addition(s) to Your Equipment List that may impact or require configuration changes to the Mobility IQ Service.
- Provide valid and applicable serial numbers for all Product problems and issues reported to Cisco or where Subscriber is seeking information from Cisco in connection with the Product use. Cisco may also require Subscriber to provide additional information in the form of location of the Product, city location details and zip code information.
- Pay all engineering time, travel, and out-of-pocket expenses if Subscriber request performance of onsite Services or Services outside the scope of Service options described in this document.
- Provide any Hardware required to perform fault isolation.
- Make all reasonable efforts to isolate the Mobility IQ Service problem prior to requesting support from Cisco.
- Acquire, install configure and provide technical support for all:

- Third-party Products, including upgrades required by Cisco or related Services; and
- Network infrastructure, including, but not limited to, local and wide-area data Networks and equipment required by Cisco for operation of Mobility IQ Service.

Data Protection Annex

This annex on the processing of personal data (this "Data Protection Annex") is supplemental to and forms an integral part of the Agreement between You ("Customer") and Cisco. To the extent Cisco, in this context, receives Personal Data (as defined below in this Data Protection Annex) from Customer and processes such data on behalf of Customer, the provisions of this Data Protection Annex apply. The scope and subject matter of processing is laid down in this Data Protection Annex, as well as in the Beta Agreement. This Data Protection Annex begins upon the commencement of the Agreement and will be in force and effect until the Agreement has been terminated or expires.

SECTION 1 INTERPRETATION

1.1. In the event of a contradiction between the Agreement, Cisco's Privacy Policy and/or this Data Protection Annex, this Data Protection Annex prevails for the subject matter indicated herein.

1.2. Terms used in this Data Protection Annex that are defined in the Agreement have the respective meanings set forth in the Agreement. The following terms used in this Annex have the corresponding definitions listed below for the purposes of the Agreement:

"**Customer Data**" means network data, including but not limited to MAC address, IP address, location information and device type, which we process in the course of making the Products available to Customer.

"**Personal Data**" means Customer Data related to a person that is identified or identifiable, as defined in the Directive 95/46/EC of the European Parliament 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 data, or any replacement legislation.

"**Sub-processor**" means any sub-contractor that processes Personal Data on behalf of Customer.

References to the Agreement will be construed as including this Data Protection Annex.

SECTION 2 ACTING AS A DATA PROCESSOR

2.1. Customer acknowledges and agrees that in the course of providing You with the Products, Cisco will be acting as a data processor (or as a Sub-processor where Customer acts as a processor of its own customer's Customer Data) on Customer's behalf in respect of the Customer Data and Customer will be a data controller under the applicable data protection laws. Customer acknowledges that Customer or Cisco is able to configure the Products so as to limit the Customer Data that is processed by Cisco.

2.2. Cisco will process and use Customer Data on behalf of Customer and only in accordance with the instructions of Customer in order to provide the Products in accordance with the Agreement, to address technical issues, in response to customer support inquiries, in accordance with any applicable end user license agreement and/or supplemental end user license agreement, and to the extent required by law. Except as described in the Agreement, the end user license agreement and/or supplemental end user license agreement, or this Data Protection Annex or as legally required, Customer Data may be processed or used for another purpose only with the prior written approval of Customer. In addition, the Customer hereby acknowledges that by virtue of using the Products, it gives Cisco instructions to process and use Customer Data in order to provide the Products in accordance with the Agreement.

2.3. Customer will comply with mandatory data protection laws applicable to Customer as a data controller in its use of the Products. Customer shall be entitled to request the deletion of Personal Data during the term or after termination of this Agreement provided that such request is reasonable, to the extent that Cisco is technically able to comply with such request without undue disruption to its business.

2.4. Cisco will comply with data protection laws applicable to Cisco as a data processor (or Sub-processor, as applicable) in providing the Products. Any Cisco obligations arising from statutory provisions or according to a judicial or regulatory decision will remain unaffected by this Data Protection Annex.

2.5. Customer acknowledges and agrees that Cisco may use the data from Customer's use of the Products in aggregate form for the following purposes: to increase Customer's visibility over data to build more context and relevance around it. Subject to the Cisco Privacy Statement at **http://www.cisco.com/web**/siteassets/legal/privacy.html, Customer hereby consents and grants to Cisco a license to collect and use Telemetry Data from the Customer. Cisco does not use Personal Data in the Telemetry Data. Cisco may share aggregated and anonymous Telemetry Data with third parties to assist us in improving Your user experience, the Products and the Software and other Cisco security products and services. Customer may terminate Cisco's right to collect Telemetry Data upon thirty (30) days written notice to Cisco.

"Telemetry Data" means samples of Company's web traffic, including data on web request attributes and information on how different types of web requests were handled by the Products. Web requests included in Telemetry Data are obfuscated to remove any Personal Data.

2.6. Customer represents and warrants to Cisco that Customer has fulfilled all the requirements under applicable data protection law (e.g. notice to and affirmative consent from data subjects) to permit Cisco to lawfully collect and use Personal Data to provide Products under the Agreement.

SECTION 3 LOCATION OF CUSTOMER DATA

3.1. Customer acknowledges and agrees that in order to provide the Products, Customer Data may be accessed and processed by Cisco or its Sub-processors in the U.S.A. Cisco and its affiliates have implemented reasonable safeguards to protect the Customer Data with regard to such processing.

3.2. Where required by the same, Cisco has entered into agreements with Sub-processors as needed to document their commitment to adequate protection of the Customer Data and authorize the onward transfer.

3.3. Cisco will not process any Customer Data outside the United States or the European Union, except for certain limited data transfers which are compliant with the EU Safe Harbor guidelines.

SECTION 4 INFORMATION AND ASSISTANCE REQUESTS

4.1. Where Customer, based upon applicable data protection law, is obliged to provide information to a data subject about the collection, processing or use of its Customer Data, Cisco shall provide reasonable assistance to Customer in making this information available, provided that (i) Customer has instructed Cisco in writing to do so, and (ii) Customer reimburses Cisco for the costs arising from this assistance.

4.2. If Cisco receives any complaint, notice, or communication that relates to Cisco's processing of Customer Data or either party's compliance with applicable law in connection with Customer 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. In providing such cooperation and assistance, Cisco will give due regard to appropriate advice that Cisco and/or the Customer receives from any relevant local data protection regulator to the extent it is applicable to Cisco's processing of Customer Data.

4.3. Cisco will, following the Customer's written request, provide to the Customer the names of its Sub-processors processing the Customer Data and the countries outside of the European Union in which such data is processed, provided that (unless it is a response to a Security Incident notified under Section 6 below) such request will not be made more than once in each calendar year.

SECTION 5 CONFIDENTIAL INFORMATION

Cisco will treat Customer Data as Confidential Information for the purposes of Section 9 of the Agreement (except that archival clauses of Section 9 will not apply to Customer Data if Customer exercises its rights in Section 9.1 below). Cisco will ensure that the employees entrusted with processing Customer Data are obliged to maintain confidentiality.

SECTION 6 SECURITY

6.1. Cisco will put in place appropriate technical and organizational measures, taking into account both the state of technologies and the costs of implementation, against unauthorized or unlawful processing of the Customer Data, and against accidental loss or destruction of, and damage to the Customer Data, including the measures set forth on Attachment 1 of this Annex (the "**Security Attachment**"). Cisco's obligations under this Article 6.1 will be satisfied by complying with terms of the Security Attachment. We regularly monitor compliance with these measures, and Customer acknowledges that Cisco may, as a part of ongoing system maintenance and development, change the appropriate organizational and technical protection measures but, in any event, the level of protection will remain appropriate as required under this clause.

6.2. Cisco maintains security incident management policies and procedures, including detailed security incident escalation procedures. If Cisco becomes aware of any unauthorized disclosure of Customer Data in breach of Section 6.1 of this Data Protection Annex (a "**Security Incident**"), then Cisco will promptly notify Customer and provide Customer with relevant information about the Security Incident, as applicable and to the extent known, including the type of Customer Data involved, the volume of Customer Data disclosed, the circumstances of the incident, mitigation steps taken, and remedial action taken and action to avoid any further incidents of that nature).

SECTION 7 AUDIT RIGHTS

7.1. Cisco will, upon request, provide Customer with a copy of any external certifications currently held by Cisco such as SSAE 16 (formerly SAS-70 Type II) or ISO 27001 reports detailing Cisco's compliance with industry information security standards.

7.2. Cisco will allow Customer to audit Cisco for compliance with the technical and organizational measures set forth in the Security Attachment if (i) Cisco notifies Customer of an actual or reasonably suspected Security Incident, or (ii) if Customer reasonably believes that Cisco is not in compliance with its security commitments under this Data Protection Annex, or (iii) if such audit legally is required by Customer's data protection law. In such event, Customer may conduct, either itself or through a third party independent contractor selected by Customer at Customer's expense, an on-site audit and review of Cisco's architecture, systems, and procedures used in connection with the relevant Product. Such audit and review may be conducted up to one time per year, with at least six week's advance written notice.

7.3. In addition, on an regular basis, Cisco will audit the security of the computing systems that Cisco uses to process Customer Data according to industry standards (the "**Cisco Audit**"), the results of which will be the confidential information of Cisco.

7.4. Upon receipt of a written request, Cisco may at its sole discretion provide Customer with a confidential copy of any report or summary produced in connection with the Cisco Audit in order that Customer may reasonably verify Cisco's compliance with the technical and organizational measures set forth in the Security Attachment.

7.5. After conducting an audit under Section 7.2 or after receiving Cisco Audit information under Section 7.4, Customer must notify Cisco of the specific manner in which Cisco does not comply with any of the security, confidentiality, or data protection obligations in this Data Protection Annex, if applicable. Upon such notice, Cisco will use commercially reasonable efforts to make any necessary changes to ensure compliance with such obligations.

7.6. Any audits described in Section 7.2 will be conducted during normal business hours, and will be of reasonable duration, and will not unreasonably interfere with Cisco's day-to-day operations. In the event that Customer conducts an audit through a third party independent contractor, such independent contractor will be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Cisco's proprietary information.

7.7. If any audit under this Article (including responding to Customer under Article 7.4) requires the equivalent of more than one business day of time expended by Cisco, Customer agrees to reimburse Cisco for any additional time expended at Cisco's then current professional services rates.

SECTION 8 SUB-PROCESSORS

8.1. Customer acknowledges and agrees that Cisco may engage its affiliates or third parties as third party Sub-processors for Cisco in connection with making the Products available to Customer from time to time.

8.2. Where, pursuant to **Section 8.1**, Cisco sub-contracts its obligations under the Agreement, it shall, prior to the disclosure of any of the Personal Data, do so only by way of a written agreement with the third party Sub-processor which imposes no less protective obligations on the third party Sub-processor as are imposed on Cisco under this EU Data Protection Annex. Where the third party Sub-processor fails to fulfil any of the EU data privacy obligations under this Annex, Cisco will remain liable to the Customer for the performance of the third party Sub-processor's obligations under that agreement.

8.3. In addition, Cisco will, upon receipt of Customer's written request, provide Customer with a list of any such third party Sub-Processors.

SECTION 9 POST-TERMINATION

9.1. On the termination or expiry of the Agreement and upon receipt of Customer's written request within three months of the termination or expiry, Cisco will use reasonable efforts to return or destroy the Customer Data, except as set forth in Section 2.5 above or where to do so would unreasonably disrupt Cisco's business operations. Where Cisco is unable to destroy the Customer Data for a legitimate reason (such as statutory obligations and/or business engagement with Customer), Cisco agrees to block such data and ensure that it is not recovered without the express written consent of Customer.

[Remainder of this page intentionally left blank]

Attachment 1

Cisco takes a systematic approach to information security and data privacy. Cisco believes a robust security and privacy program requires active involvement of stakeholders, ongoing education, internal and external assessments, and instilment of best practices within the organization.

The following measures underlie Cisco's systematic approach to information security and data privacy. Collectively, these measures include controls:

- to prevent unauthorized access to data processing systems in which Customer Data is processed (**admittance control** and **physical access control**); Examples include:

    - secure account credentials
    - account security protections (strong passwords, password expiration and rotation, maximum number of failed attempts, IP-based login restrictions, etc.)
    - change management including change logs and change event alerting
    - 24x7 automated intrusion detection

    - A high security card key system and biometric readers are utilized to control facility access
    - All entries, exits, and cabinets are monitored by video surveillance
    - Security guards monitor all traffic into and out of the datacenters 24x7, ensuring that entry processes are followed
    - software development life cycle and change management / change control policy and processes
    - product development secure coding guidelines and training policy and procedures
    - access to Customer data restricted to personnel based on appropriate business need and limited by functional role

- to prevent data processing systems from being used without authorization (**access control**). Examples include:
    - software development life cycle and change management / change control policy and processes
    - access to Customer data restricted to personnel based on appropriate business need and limited by functional role
    - information security responsibilities for employees
    - audit trails policy and procedures, and history & log retention policy and procedures [bu to put a policy into place]
    - data control & access control policies and procedures

- to ensure that persons authorized to use systems in which Customer Data is processed only have access to the Customer Data as they are entitled to in accordance with their access rights and authorizations, and to prevent the unauthorized reading, copying, modification or deletion of Customer Data (**data access control**); Examples include:
    - access to Customer Data restricted to personnel based on appropriate business need and limited by functional role
    - audit trails policy and procedures, and history and log retention policy and procedures

- to prevent the unauthorized reading, copying, modification or deletion of Customer Data which is under Cisco's control while Customer Data is being transferred electronically, transported or recorded on data storage devices, and to ensure that the intended recipients of Customer Data who are provided with Customer Data by means of data communication equipment can be established and verified (**data transfer control**); Examples include:
    - encrypted communication between Cisco Hardware devices and Cisco's servers (HTTPS / SSL), as well as between Cisco's servers
    - logging of activity of administrators (time, IP, and approximate location (city, state) of logged in administrators)
    - Accounts passwords stored in encrypted format on Cisco servers

- to ensure it is possible to establish an audit trail as to if and by whom Customer Data have been entered into, modified in, or removed from systems being used by (or on behalf of) Cisco to process Customer Data (**input control**); Examples include:
    - logging of activity of administrators (time, IP, and approximate location (city, state) of logged in administrators)

  - access to Customer data restricted to personnel based on appropriate business need and limited by functional role
  - data control & access control policies and procedures
- to ensure that Customer Data processed by or on behalf of Cisco can only be Processed in accordance with the Customer's Instructions (**order/instruction control**); Examples include:
  - change management including change logs and change event alerting
  - audit trails policy and procedures, and history & log retention policy and procedures
- to ensure the protection of Customer Data which is under the control of Cisco against accidental destruction or loss (**availability control**); Examples include:
  - Real-time replication of data between datacenters (within 60 seconds)
  - Nightly archival backups

- to ensure that Customer Data collected is only used for the intended purpose under the Agreement (**intended use control**). Examples include:
  - Customer Data is automatically processed only according to the terms of the Agreement
  - change management including change logs
  - audit trails policy and procedures, and history & log retention policy and procedures

Additional measures include the following:

Out-of-Band Architecture
- Only network usage statistics are stored in the cloud
- Data stored or transmitted by means of Customer's network does not traverse Cisco's servers

Cloud Services Security
- Daily vulnerability testing of datacenter infrastructure
- Protected via IP and port-based firewalls
- Remote access restricted by IP address and verified by public key (RSA)
- Systems are not accessible via password access
- Administrators automatically alerted on configuration changes

Cloud Services Infrastructure
- datacenters are certified by industry-recognized standards including SSAE16, ISAE 3402 (SAS-70) including Type II, ISO 27001:2005, or ISO 27001.
- configuration standards for all system components policy and procedures
- 24x7 automated failure detection — all servers are tested every five minutes from multiple locations

Disaster Preparedness
- Datacenters feature sophisticated sprinkler systems with interlocks to prevent accidental water discharge
- Diesel generators provide backup power in the event of power loss
- UPS systems condition power and ensure orderly shutdown in the event of a full power outage
- Each datacenter has service from at least two top-tier carriers
- Seismic bracing is provided for the raised floor, cabinets, and support systems
- In the event of a catastrophic datacenter failure, services fail over to another geographically separate datacenter

Organization and Personnel
- formal assignment of information security responsibilities by the Chief Information Security Officer (CISO) and the Cisco Security Team
- a formal security awareness program
- documentation and business justification for use of all services, protocols and ports allowed
- management of service providers policy and procedures
- background review of all Cisco personnel
- Rapid escalation procedures across multiple operations teams