Service Description

Cisco Managed Service

This Service Description is part of the Services Agreement (as defined in the Services Guide) and describes various Services that Cisco will provide to You. Capitalized terms, unless defined in this document, have the meaning in the Services Guide.

1. Summary

- The Cisco Managed Service ("**Services**") are a set of multi-technology managed services that consist of the monitoring, management, and troubleshooting of Managed Elements identified in a Quote. The Services components are based upon practices recommended by the Information Technology Infrastructure Library (ITIL).
- The Services include access to a portal ("**Portal**") to allow Customer to view reports and other Services-related information and submit Service Requests.
- Services components associated with specific technologies (e.g., networking, data center, collaboration, and/or security) or supplemental services purchased by Customer are described in one or more supplements to this Service Description (each, a "**Supplement**") and referenced in the Quote.
- Unless otherwise described in the Quote or stated below, all Services are delivered remotely from Cisco's global data centers and Network Operations Centers (NOCs) and are monitored 24x7x365.

Summary of Services

Core Services	Optional Services (if purchased)
• Service Transition and Activation. • Managed Element Inventory • Configuration Backup and Restoration • Event Management • Incident Management • Change Management • Problem Management • Service Delivery Management • Service Delivery Reporting • Exit Assistance	• On-Premises Cisco Managed Service Platform Appliance(s) and Optional Geo-redundancy • Smart Bonding for Cisco Managed Service • Service Request Fulfilment • Management of Third-Party Managed Elements • User Access Management • Carrier Management

2. Core Services

2.1 Service Transition and Activation

Cisco and Customer define the plan for establishing connectivity between Cisco and the Managed Elements. The parties connect the Managed Elements to the Cisco Managed Service Platform, through a VPN endpoint provided by Cisco. Cisco then performs tests to confirm that the Managed Elements are ready for remote management ("Activation," "Activate," etc.). Cisco also provides Customer with a draft of a Runbook with Customer provided information (e.g., Customer contacts, etc.) for Customer's input.

Accompanying Tasks
• Cisco creates a Service Activation Plan which defines the scope of work required to transition the in-scope Devices to be Activated as a Managed Element, including required inventory information and topology requirements, assessing stabilization activities required to the Devices and Network. • Customer reviews and approves the Services Activation Plan, including Activation date(s). • Customer promptly provides Cisco with remote access and control to the Managed Elements and requested inventory and topology information. • Parties perform any other tasks designated as its responsibility in the Services Activation Plan (e.g., Customer stabilization activities, sharing port requirements, etc.) by the date specified in the Services Activation Plan. • Customer installs and configures VPN endpoint (with Cisco assistance) using Cisco-provided instructions. • Cisco Activates and/or decommissions Managed Elements, per the applicable Quote(s) and Customer guidance. • A detailed deliverables and responsibility matrix is captured as part of Service Transition and Activation, including a process from Day-1 (Devices under deployment and not operational yet) to Day-2 (Deployed, tested, in production, and Operational) handover for new devices. This ensures that devices are appropriately onboarded and tested for operational readiness. • Cisco creates the draft Runbook describing operational processes applicable to the Services including, backup and restore, event management, incident management, change management, Service Delivery reporting and exit assistance.
Output: Services Activation Plan, Draft Runbook, initial Managed Element inventory, and Change Request, if needed

2.2 Managed Element Inventory

Cisco Team collects and maintains inventory of all Managed Elements from the Cisco Managed Service Platform. Cisco makes this information available to the Customer via a web-based Customer Portal which can be accessed by the Customer.

Accompanying Tasks
• Cisco maintains the inventory of Managed Elements, including any additions or deletions. • Cisco maintains Customer access to the inventory of Managed Elements via the Portal. • Cisco supports in true up process with Customer. • Customer provides Cisco with a single point of contact for all technical support matters as they relate to the Managed Elements.
Output: Managed Element inventory.

2.3 Configuration Backup and Restoration Services

Cisco performs a periodic backup of the configuration settings of the Managed Elements. Cisco does not back up any other data relating to the Managed Elements including, without limitation, any content or applications. The periodicity, method and mechanisms used to perform the backup activities varies by technology. Cisco and Customer address these matters during the Service Transition and Activation activities and Cisco documents the outcome of these discussions in the Runbook. Depending on the connectivity type and the Managed Elements, Customer may be required to provide storage. Cisco restores this data in response to an Incident or as a part of Service Request Fulfilment.

Accompanying Tasks
• Cisco documents the periodicity, method and mechanisms used to perform the backup activities in the Runbook, after consultation with the Customer during Service Transition and Activation. • Customer configures the Managed Elements to allow back-up of the settings of the Managed Elements, with Cisco's guidance. • If Cisco detects an automatic back-up has failed, it attempts to manually rerun the back-up. If Cisco detects continued backup failures, it notifies Customer and Cisco creates an Incident ticket.

• Customer backups the Managed Elements that Cisco cannot backup (e.g., Third-Party Managed Elements). • On Customer’s written request, Cisco provides a report of the Managed Elements being backed up and copy of the backup settings.
Output: Backup of settings of Managed Elements.

2.4 Event Management

Cisco monitors the Managed Elements for Events.

Accompanying Tasks
• Cisco creates and maintains Event Management policies (e.g., Event thresholds) in consultation with Customer. • Cisco monitors the Managed Elements for Events by monitoring syslog, SNMP trap messages, Key Performance Indicators (KPIs), and/or Threshold Crossing Alerts (TCAs) from Managed Elements. • Cisco helps to identify meaningful Events by implementing Event correlation, timing, and filtering processes when an Event occurs. • If an Event becomes an Incident, Cisco creates an Incident ticket and perform Incident Management activities described below in **0** • **Incident** Management**.**
Output: Platform enablement to support automated and correlated Incident, Problem and Change Management events.

2.5 Incident Management

If an Incident is proactively detected by Cisco Managed Service Platform or reactively reported by the Customer, Cisco creates an Incident ticket, classify (or reclassify) the Incident, notify and update Customer, and work to identify, troubleshoot, and restore normal operational functionality of the Managed Elements (which may include a temporary workaround). An Incident is considered restored once the Managed Element operates normally again or Cisco provides a restoration recommendation to Customer.

Accompanying Tasks
• Cisco monitors the Incident ticket queue on Cisco Managed Service Platform and acknowledges the incident automatically or manually. • Cisco assesses and re-assigns the priority of the Incident, if required. • Parties promptly review and approve proposed Changes to resolve an Incident. • If the cause of an Incident is out of scope or out of Cisco’s control, Cisco notifies Customer with recommendations to help resolve the Incident. • Customer may be required to perform the portions of the Changes if Cisco cannot (or does not have permission to) perform the Changes or if the Changes are out of scope (e.g., a Change required to out of scope software, or the Change requires on-site intervention).
Output: Incident Ticket, Change Request for Incident restoration; Recommendation for Incident restoration.

2.6 Change Management

Cisco manages the lifecycle (i.e., planning, review, backout, and post-change checks) of the deployment of technical changes (e.g., configuration changes) to the Managed Elements. Change types supported by Change Management are Emergency Changes (Changes done to retore services or prevent outages), Normal Changes (Non-emergency service requests), Custom Scoped Changes (Undefined changes), Standard Changes (Tested and pre-approved Service Requests).

Accompanying Tasks
• The parties review, validate, approve, and prioritize Change Requests based on urgency. • Cisco participates in Customer Change Advisory Board (CAB) meetings (max. 2 hours per week), as they relate to the Managed Elements. • Parties perform tasks, agreed to in writing during the CAB meeting and follow the Change Management Process as described in the Runbook. • If Cisco is unable to perform all elements of the Change remotely, Customer assists Cisco in performing the Changes (with Cisco guidance). • Customer reviews and mitigates any impacts to monitor-only or out-of-scope Devices as a result of any Changes to the Managed Elements.

Accompanying Tasks
• Details of change management process are captured during the Service Activation and documented in the Runbook.
Output: Recommendations for Change; Change Requests; Change Plan; Change Record.

2.7 Problem Management

Cisco involved problem management in two scenarios:

1. After restoration of an Incident, Cisco works to identify a root cause for P1 Incidents under a reactive problem ticket. The reactive problem ticket is analyzed using the historical root cause information, analytics, known error databases, and other tools to determine the underlying root cause of the incident and prevent the incident from repeating.
2. Cisco performs proactive chronic checks (incidents trends, repetitive), PSIRTS, Field Notices and Defects on managed devices and device families through proactive problem ticket to prevent from any incident causing major outage.

Accompanying Tasks
• Cisco reviews Cisco PSIRT High and Critical notifications, Cisco security vulnerabilities, Known Error databases, and field notices against Customer Problem records. • Cisco provides actionable recommendations to Customer to resolve the Problem and reduce or eliminate Incidents resulting from that Problem. • Parties implement Changes to resolve problems according to Change Management. • Customer manages and address third-party suppliers and out of scope sources of Problems. • Cisco submits Initial RCA documents for P1 incidents within 5 Business days from the restoration.
Output: Change Request; Change Record; Problem Record; recommendations to resolve Incident or Problem.

2.8 Service Delivery Management

To help support the delivery of the Service and confirm that service delivery processes are in place, Cisco provides Service Delivery Manager as a primary point of contact for the Cisco Managed Service.

Accompanying Tasks
• Customer is assigned with complementary single points of contact for Services receipt and coordination. • Cisco provides an agenda and host monthly operational meetings to discuss items such as, Tickets and reports, SLA performance, suggested Changes, etc.). • Cisco also provides an agenda and host quarterly review meetings to discuss items such as, Problems, Services improvement recommendations, and Services alignment to Customer's strategy and priorities. • Cisco updates the Runbook in response to material changes, with Customer input. • Each party performs assigned tasks resulting from meetings, as mutually agreed in writing.
Output: Recommendations, meeting agenda, draft Change Requests, performance reports.

2.9 Service Delivery Reporting

Cisco shares a predefined set of IT Service Management (ITSM) reports of the Managed Elements through Services Portal.

Accompanying Tasks
Cisco enables the following ITSM reports via the Portal. • Service Level Management. • Incident Management Report. • Problem Management Report. • Change management reports. • Updated inventory list as available in CMDB through Cisco Managed Service Platform. Cisco highlights if there is a major deviation on the Incident, Problem and Change trend or service level performance deviation.
Output: Service level management data to measure delivery performance.

2.10 Exit Assistance

Cisco assists Customer in transitioning the Services back to Customer or to Customer's third-party provider by making available Customer materials as received from Customer in transition phase or during operations, providing knowledge sharing sessions, and removing access to and deleting Customer data stored on its Cisco Managed Service Platform.

Accompanying Tasks
• Cisco makes available the Runbook, Ticket data, reports, and available Managed Element inventory and technical documentation received during transition phase. If desired, Customer can download this data or request it, if it is not available on the Portal. • Cisco disconnects the Cisco VPN from Customer and confirm disconnection via email to Customer. • Customer removes any Cisco access to Customer's systems or Managed Elements. • Cisco provides up to 3 virtual knowledge transfer sessions on the processes and data being handed over. • Cisco deletes Customer Data and unaggregated Operations Data from Cisco Managed Service Platform within 60 days of termination or expiration. • Customer promptly returns any Cisco-provided hardware or software. Customer is responsible for any loss, theft, or damage to these items until returned.
Output: Copy of Runbook, topology documents; copies of Reports. Maximum of 3 virtual knowledge sharing session 2 hrs each.

3. Optional Service Components

The following Services components are optional and may be purchased as additional Services and are subject to additional Charges unless the Quote lists them as included with the Services.

3.1 On-Premise Cisco Managed Service Platform Appliance(s) and Optional Geo-redundancy

Cisco provides and maintains one or more (as provided in Quote) Cisco appliance(s) as Data Collection Tools for use at Customer site(s). These appliances may replace a cloud hosted Cisco Managed Service Platform or can be a supplement to the cloud hosted Cisco Managed Service Platform as provided in the Quote.

Accompanying Tasks
• The parties agree on appliance location(s) and priority (e.g., main, and secondary). • Customer installs, configures, and maintains (e.g., power, HVAC, connectivity etc.) appliances according to Cisco provided requirements and documentation, including connectivity between the appliances and the Managed Elements. • Cisco provides remote technical support to aid in troubleshooting any issues or errors of the above Customer activities. See Service Transition for additional information. • Cisco maintains the appliance (e.g., software updates, configuration changes, etc.) and provide refreshed appliances as needed. • Customer makes change/maintenance windows available and perform requested changes to the appliances, associated network connections or Managed Elements that Cisco cannot perform remotely. • If there is an outage impacting one appliance, Cisco updates network configurations to route network traffic to an available Cisco Managed Service Platform instance (based on configuration).
Output: Cisco Managed Service Platform Tools and remote guidance for installation, Services Activation Planning, and support services.

3.2 Smart Bonding for Cisco Managed Service

Cisco provides Cisco Managed Service Platform integration points to allow Customer’s ITSM system to communicate with the Cisco Managed Service Platform to facilitate the exchange of tickets, status updates, workflow processes, and similar information (Smart Bonding). The extent and type of the integration is documented in the Quote or mutually agreed in writing. Smart Bonding is limited to a single integration between Cisco’s Cisco Managed Service Platform and Customer’s ITSM. Smart Bonding is highly recommended.

Accompanying Tasks
• If not provided in Quote, the parties agree an integration plan, data exchange types (e.g., one or bi-directional, which data categories) and a test plan. • Cisco provides ITSM integration interface (e.g., APIs), specifications and documentation to allow the integration between the Cisco Managed Service Platform and Customer’s ITSM. • Unless otherwise provided in writing, Customer configures and maintains Customer’s ITSM system to interoperate with Cisco Managed Service Platform API interface. Cisco provides reasonable troubleshooting support for the Integration. • If changes to the Cisco Managed Service Platform require the update to the integration, Cisco notifies Customer, provide updated APIs and documentation, and assist Customer in testing and troubleshooting the updated integration. • The Smart bonding is done and tested during Service Transition and Activation.
Output: Integration and API specifications and documentation; test plan.

3.3 Service Request Fulfilment

The Portal allows Customer to view the Service Catalogue and request, categorize, approve, prioritize, check status of, and obtain reports on, Service Requests. Upon receipt and qualification of a Service Request through the Portal, Cisco implements Service Requests, consuming the number Service Request Units (SRUs) as provided in the Service Catalogue. Cisco separately scopes and quotes Service Request types not in the Service Catalogue and get approval from Customer before proceeding.

Accompanying Tasks
• Customer provides a list of authorized requestors that may submit Service Requests (“SR”) on the Portal. • Cisco manages submitted Service Requests through the SR lifecycle-e.g., receipt, validation, approval, completion, closure, notifications, and updating documentation in conjunction with Change Management process. • Customer submits requested information to validate a Service Request. Failure to submit all needed information may result in a delay.

• If requested by Cisco, Customer acknowledges when the Service Request is completed. • Cisco handles urgent Service Requests per the Service Catalogue.
Output: Service Request reporting, Service Request catalogue, and Change Request.

3.4 Third-Party Managed Elements

Cisco manages Third Party Managed Elements expressly identified in the Quote. The Quote identifies the Service components that Cisco provides for the Third-Party Managed Elements. If not specified in the Quote, Cisco's Managed Services are limited to Monitoring, Incident, and Change Management, but only to the extent that the Third-Party Managed Element is compatible with Cisco's Cisco Managed Service Platform and relevant software updates are available to Cisco.

Accompanying Tasks
• Customer provides Cisco a valid Letter of Agency (LOA) and maintain valid support and maintenance contracts with third party suppliers of Managed Elements. • Customer is responsible for managing security-related notices or Incidents for Third Party Managed Elements.
Output: Letter of Agency.

3.5 User Access Management

Cisco uses Customer's multi-factor authentication methods and processes for Cisco's access to the Managed Elements.

Accompanying Tasks
• Customer provides Cisco-requested authentication technology (including any hardware or software), documentation, any required licenses, and reasonable remote assistance to implement it. • Cisco provides Customer with a list of Cisco users, along with the users' Cisco email addresses. • Upon written request, each party provides the other party with reports associated with authorized users. • Cisco notifies Customer when user credentials need to be revoked and Customer promptly revokes that user's access. • Upon termination or expiration of the Services, Cisco discontinues use, and return or delete any hardware or software provided by Customer for authentication purposes. • Cisco ensures to protect any Personal Identifiable Information (PII) data of the Cisco users.
Output: Cisco access lists and logs, Enhanced Authentication software, hardware, documentation and/or requirements (all as applicable).

3.6 Carrier Management

The purpose of Carrier Management is to enable Cisco to serve as a representative of Customer with Customer's circuit providers (Carrier). In order for Cisco to perform the activities described, Customer must execute a LOA (Letter of Agency) granting Cisco permission to do so on Customer's behalf. Cisco manages Customer's existing circuits as well as those newly provisioned circuits as may be agreed in writing between Customer and Cisco. Circuits to be managed are documented during the service activation and activation with required details.

Accompanying Tasks
Cisco performs the following tasks: • Coordinates reactive circuit maintenance notifications from carrier provider. • Engages the responsible Carrier, as necessary, to resolve circuit-related Incident(s). • Engagement occurs in the local language of the Carrier if contracted. • Triages and escalates problems to Customer support staff and/or responsible Carrier. • Escalates Incidents in collaboration with Customer. • Works with Customer to perform regular review with Carriers for service improvements. • Provide a SPOC for Carrier Management 8x5 support. • provide Dedicated 24x7 Carrier Network Engineers (CNE) support model. Customer performs the following tasks: • Provides Cisco with a valid LOA that has been accepted by the responsible Carrier. • Negotiates and executes valid contracts with Carrier(s), including SLAs. • Provides Cisco with copies of valid contracts with Carrier(s) or a suitable summary of the necessary and relevant operational sections of such contracts. • Enforces any contract terms in the event of a default by the Carrier(s) as determined by customer. • Conducts all commercial discussions for new orders, renewals, upgrade, and demise with the Carrier(s).
Output: Carrier Performance Scorecards, Loss of Resilience Reports, Automation capabilities Dashboards.

Exhibit A

Managed Services Terms

1. Services Terms

1.1 Scope of Additional Services

Unless the Services are expressly provided for above, or described in the Quote or service catalogue, all other Cisco services are out of scope for this Service Description. Customer will manage all products and/or services that are not in the scope of Services (including the associated impacts from the Services).

1.2 Managed Elements

a. As part of Service Transition, Cisco describes any limitations of the Services with respect to the Managed Elements, if applicable. For example, certain Third-Party Managed Elements may only be monitored for availability (sometimes called "up/down") with limited additional Services provided.

b. Cisco does not provide Services for any Managed Elements that are unauthorized (e.g., grey market) or LDOS, unless expressly provided in the Quote(s).

c. Any incidental management of Devices (i.e., those Devices not considered Managed Elements) by Cisco is without any warranties or continuing obligations of any kind.

d. Customer must maintain a valid Cisco license and support and maintenance agreement for all Managed Elements. Cisco reserves the right to charge Customer the equivalent support and maintenance fee for those Managed Elements that are not covered, or may reduce the Services (e.g., Cisco does not install updates, submit requests for hardware replacement, etc.) for those Managed Elements that do not have a valid Cisco support and maintenance agreement.

e. Customer must use the Managed Elements according to their applicable licenses, specifications, and documentation (e.g., do not exceed available capacity on a Managed Element). Customer provides and maintain sufficient connectivity (including, without limitation, any required local circuits, cross connects, and hardware) to Cisco's NOC.

1.3 Reporting

Cisco provides, or makes available via the Portal, the reports listed in the reporting documentation for Cisco Managed Service. Cisco reserves the right to add, change, or remove Reports in its reasonable discretion. Customer may review any reports with Cisco as a part of Service Delivery Management. Customer should notify Cisco within a reasonable timeframe if Customer believes a report is inaccurate.

1.4 Portal

Cisco provides a web-based Portal that provides Customer at least the following core functionality:

a. Review of Reports and information related to the Services.

b. Ability to submit and monitor Incident Tickets; and

c. Ability to submit and monitor Service Requests (see **3.4 Third-Party Managed Elements** above)

Requests submitted by Customer's requestors are deemed to be authorized by Customer.

1.5 Cisco Managed Service Platform

The Cisco Managed Service Platform is the system of record for the Services. Unless Customer only uses the On-Premises Cisco Managed Service Platform Service component, the Cisco Managed Service Platform uses cloud-based services to process Managed Element data and provide the Services. These components are hosted in a secure data center with at least one redundant system. Cisco is responsible for maintenance of the Cisco Managed Service Platform.

1.6 Cisco Recommendations and Changes

If Customer fails to implement any requested Cisco recommendations or requirements or fails to allow Cisco to make recommended Changes with respect to the Managed Elements or the Services, Cisco shall have no responsibility for any resulting delays, failure(s), or increased security risks with respect to the performance of the Managed Elements or Services. In addition, if Customer's failure to implement Cisco's reasonable recommendations or its unreasonable refusal to allow Cisco to make Changes causes Cisco to incur more costs or effort to provide the Services (e.g., significantly increased number of Incidents), Cisco may charge additional charges to address such items until the recommendations are implemented.

1.7 Governance

In addition to Service Delivery Management, Cisco and Customer implement a governance function with the following goals: discuss alignment of the services to Customer's business needs and this Service Description, identify opportunities to improve the Services (e.g., increase quality or reliability), resolve disputes, highlight new Cisco technologies, any Services renewals, or extensions, identify market and technology trends related to the Services and similar matters. Cisco provides an agenda and host remote quarterly governance meetings to discuss the above items.

1.8 Technical Support

Cisco operates on Customer's behalf to request replacement hardware or software and helps coordinate the delivery of the replacement Managed Components to Customer.

1.9 Training and Policies

a. Cisco personnel requiring to access any Customer site(s), Managed Elements, or other Customer systems remotely participates in any reasonable Customer-requested training (up to a maximum of 6 hours per year) without additional Charges.

b. Cisco materially complies with Customer's reasonable written security policies applicable to the Services provided that: (a) the policies are in writing and provided to Cisco reasonably in advance of the requested compliance date; (b) Cisco has sufficient control to implement the polices; and (c) the policies do not conflict with Cisco's policies, amend or conflict with the Agreement or this Service Description, change the allocation of risk or liability between the parties, increase the scope of Services, or cause Cisco to incur increased risks or costs to comply with such policies.

c. If customer requires personally identifiable information of any Cisco Personnel to be provided access to Customer's systems or Managed Elements, Customer must provide this request to in writing promptly after the effective date of its policy and maintain a privacy and security program to protect Personnel's information at least as robust as the privacy and security obligations Cisco provides Customer regarding personal information, or the obligations at the following if none are in the Agreement: Trust Center.

1.10 General Customer Responsibilities

Cisco's provision of the Services is dependent on Customer's compliance with its responsibilities as listed in this Service Description and those responsibilities described in the Services Guide. If Customer fails to perform its responsibilities or if an exclusion (listed in Section 1.11 below) applies, Cisco is excused from performing the Services (including achieving any Service Levels) to the extent, and for the duration that Customer's failure to meet its responsibilities reasonably prevents Cisco from performing its responsibilities. In addition, Cisco reserves the right to charge Customer for expenses, costs, or time incurred, caused by Customer's failure to perform its responsibilities.

1.11 Exclusions

Products and services that are not described in this Service Description are not part of the Services, including, but not limited to, the following examples:

a. Services or software to resolve any Incidents or Problems resulting from an unmanaged third-party product or causes beyond Cisco's control unless specified otherwise in the applicable Quote(s);

b. Software or hardware upgrades or updates unless in response to an Incident or Problem, or unless expressly referenced in this Service Description, Supplement(s) to this Service Description, or the applicable Quote(s);

c. Unless provided for in a Quote, providing Services onsite or in any language other than English; and

d. Troubleshooting Incidents that predate Service Activation.

e. Cisco does not provide services for any Managed Elements that are EoX (e.g., End of Life, End of Support, etc.) unless expressly provided in the applicable Ordering Document(s).

2. Commercial Terms

2.1 Pricing Summary

The charges for the Services ("Charges") and payment terms are detailed in the Quote or Agreement. Except as provided in the Quotes or Agreement, all Charges paid are non-refundable.

2.2 Invoicing

a. If Customer has elected to prepay for the Services, Cisco invoices Customer on or after the effective date described in the applicable Quote (the "Effective Date").

b. If the Charges include Service Activation Charges, Cisco invoices those Charges on or after the Effective Date. Except for material breach by Cisco, Service Activation Charges are non-refundable.

c. If no invoicing terms are provided in the Quotes, the Charges are pro-rated for the number of years of the term and paid annually in advance.

d. If the Quotes provide for invoicing upon Service Activation, Cisco begins invoicing on Service Activation Date.

e. Cisco's rights to invoice for the charges for the Services and Customer's obligation to pay is not affected by (i) any delays caused by Customer (or anyone acting on Customer's behalf), (ii) Customer's failure to perform or delay in performing its obligations under this Service Description or any Supplement, or (iii) Customer's failure to issue a purchase order.

2.3 Minimum Commitments and Minimum Term

The Quote contains any minimum term or minimum Charges commitment associated with the Services.

2.4 Service Activation

The Services Activation date is the date provided in the Services Activation Plan. Unless expressly covered in the Quote, Service Activation dates more than ninety (90) days from the Effective Date may incur additional Charges. If Customer causes the delay in Service Activation, the Services are deemed Activated on the original planed Services Activation Date. If no date is listed in the Services Activation Plan, the Service Activation Date is as the Managed Elements are Activated, or ninety (90) days from the effective date of the Services, whichever happens first.

2.5 Additional Devices Added as Managed Elements

If Customer makes any change to the number or type of Managed Elements from those Managed Elements quoted/priced in the applicable Quote, the monthly Charges for the Services are adjusted accordingly. If Customer wishes to add new Devices as Managed Elements and there is no true-up, audit, rate card, or similar provision in the Quote, the parties follow Cisco's standard change request process ("**Change Request**").

2.6 Service Request Charges and Service Request Units (SRUs)

Customer's applicable Quote(s) lists the aggregate number of SRUs included in the Service purchased. If Customer uses all the available SRUs, then Customer may purchase additional SRUs. SRUs are not refundable and must be used during the term listed in the applicable Quote or they expire. Cisco invoices Customer for the remainder of the Charges for any Service Requests that are fulfilled by Cisco during the applicable billing month if Customer does not enough SRUs.

2.7 Term, Termination, and Renewal

(A) Term

The term of the Services is provided in the Quotes. Unless provided in the Quotes, the Term begins upon the Effective Date of the Quote.

(B) Termination

Where a Quote contains a minimum commitment or contract value, if Customer terminates the Services for convenience, Customer pays remainder minimum commitment or contract value due under the Quote. If the Quote does not contain a minimum commitment, Customer may not terminate the Services for convenience, even if the Agreement allows it, unless expressly provided in the Quote. Rights to terminate for material breach are provided in the Agreement.

(C) Renewal

The Service automatically renews for additional one-year terms at the same price, unless Cisco notifies Customer in writing at least ninety (90) days in advance of, or Customer notifies Cisco in writing at least forty-five (45) days in advance of, the expiration of the then-current term that it does not want to renew the Services.

3. General Terms

3.1 Related Documents

This document should be read in conjunction with the following documents: (1) Glossary of Terms for the Service Description for Cisco Managed Service (available at Service Descriptions); (2) any Service Level Agreement referencing this Service Description; (3) the methodology and associated terminology used in determining the priority level of an Incident, which is included in this Service Description; (4) the Services Guide; and (4) any Quote(s).

3.2 Order of Preference

If there is a conflict between this Service Description, an Quote, the applicable Agreement the Services Guide, or any Supplement to this Service Description, the following priority applies (from highest to lowest): (a) any Quote, as applicable; (b) any Supplement(s); (c) the Service Description; (d) the Services Guide; and (e) the applicable Agreement.

3.3 Confidential Information

The Runbook, Charges, Portal, Data Collection Tools (including Cisco Managed Service Platform), and Service Level performance information, excluding Customer's data, are Cisco Confidential information. This information may not be used for any purpose other than in connection with Customer's use of the relevant services provided by Cisco.

3.4 Personal and non-Personal Data

For details on what data Cisco collects from Customer in connection with the Services, refer the Cisco Managed Service Privacy Data Sheet.

Exhibit B

Priority Levels

This Exhibit B describes the methodology used in determining the priority level of an Incident. Cisco classifies Incidents according to "Impact" and "Urgency" and then defines the Priority of the Incident by applying the Impact and Urgency terms to the chart below.

Impact	Urgency
An Incident is classified according to the breadth of its impact on Customer's business (the size, scope, and complexity of the Incident).	The Urgency of an Incident is classified according to its impact on the Services or ability for Customer to receive the Services and the financial impact to Customer's business.
There are four impact levels: • **Widespread:** Entire Service or multiple regions are affected • **Large:** Multiple locations are affected • **Localized:** A single location or individual users at multiple locations are affected • **Individualized:** A single user is affected	There are four urgency levels: • **Critical:** Primary function is stopped with no redundancy or backup. • **Major:** Primary function is operating but degraded. • **Minor:** Non-Primary function is stopped or severely degraded. • **Low/Notice**: Non-critical business function is degraded. There is no material impact.

Priority Definitions

Priority defines the level of effort that is expended by Cisco and Customer to resolve the Incident. The Priority level is determined by applying the Impact and Urgency definitions to the chart below.

IMPACT					
URGENCY		Widespread	Large	Localized	Individualized
	Critical	P1	P1	P2	P2
	Major	P1	P2	P2	P3
	Minor	P2	P3	P3	P3
	Low/Notice	P4	P4	P4	P4

Notes:

- Cisco adjusts the case priority in accordance with updated Priority of Impact or Incident resolution.
- Customer requests to escalate Incidents to a higher priority than their 'natural' classification may incur additional Charges.
- Ticket (case) may be left open for a prescribed period after restoration or Change completion while operational stability is being assessed.
- Cisco's Incident Management priorities below are contingent on necessary Customer assistance or information to resolve the Incident.

  Cisco Incident Management priorities are defined as follows:

  - P1-P2 Cisco and Customer commit all reasonable resources 24x7 to resolve the situation.
  - P3-P4: Cisco and Customer are willing to commit reasonable resources during Standard Business Hours to restore service to satisfactory levels.