CENTURYLINK INFRASTRUCTURE & APPLICATION MANAGEMENT SERVICES
SERVICE GUIDE FOR CROSS FUNCTIONAL SERVICES

This Service Guide ("SG") sets forth a description of the Cross Functional services ("Services") for CenturyLink Infrastructure & Application Management Services, including technical details and additional requirements or terms, if any. This SG is subject to and incorporated into the governing agreement and SOW between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant SOW. CenturyLink and Customer responsibilities, respectively and service description terms are set forth in this SG.

SERVICE DESCRIPTION

Cross Functional Services are a set of ITIL processes that will apply to the delivery of all Services delivered by CenturyLink through the Remote Infrastructure Management Operations SOW (the "Operations SOW"). Services described in this Service Guide will refer to the various functions specified below to be provided to Customer by CenturyLink. The Cross Functional Services available to Customer include:

- Event Management
- Incident Management
  - Critical Incident Management
  - Security Incident Management
- Problem Management
- Release Management
- Change Management
- Service Requests
- Availability Management
- Capacity Management
- Performance Management
- Asset Management

Central management, reporting, and tracking are also provided for the Services. CenturyLink has fully adopted and integrated the IT Infrastructure Library (ITIL) framework. This framework provides the structure for the methods and procedures used to deliver operational services to Customer.

EVENT MANAGEMENT

CenturyLink will provide Event Management Service to Customer, which will enable the detection of performance or service-impacting conditions within the supported environment. Event Management ensures that performance or service-impacting conditions are not only detected, but also reported and appropriately acted upon to ensure efficient problem resolution.

The Event Management function includes the following seven components that will be performed by CenturyLink:

- Event Detection - An Event is defined as a significant occurrence that represents either a deviation from normal operations or a change in the status of a Configuration Item (CI). When an Event occurs, notification messages are detected by monitors that act on the Event by performing prescribed actions or sending data about the Event to a central event-monitoring console where it is reviewed and acted upon by Event Management personnel.
- Event Filtering - After an Event is detected, it will be filtered to determine if it should be communicated to the Event Management tool or ignored. Event Filtering may also determine that only the first Event will be transmitted when a series of repeated or subsequent Event notifications occur. In addition, Event filtering will perform the first level of correlation to determine if the Event is informational, a warning, or an exception.
- Event Logging and Categorization - The Event is logged as an Event Record in the Event Management tool. In some instances, the Event will simply be left as an entry in the system log of the device or application that generated the Event.
- Event Correlation - Event Correlation is performed by a correlation engine that compares the Event with a set of criteria and rules in a prescribed order to determine the level and type of business impact and identify possible responses.
- Evaluate and Trigger - Evaluation determines the Event's business impact based on Service Level targets and checks the availability of prescribed actions to resolve the Event. If a response or action is correlated, the corresponding trigger is initiated.
  - If correlation determines that a Change is appropriate, the Change Trigger will be initiated to submit a SOW Change Request.
  - Similarly, if appropriate, an Incident Trigger can open an Incident Record, or a Request Trigger can submit a Service Request.
  - If an automated action is available for an Event, the trigger will initiate the action and then evaluate the action to verify successful completion. If the action fails to resolve the situation, an Incident Record will be created.

- Human Intervention - Events that have not been responded to will be escalated for further investigation and human intervention. A central Event Management tool will be used to display and control escalated Events.

Review Events - Events reviews are performed regularly and are comprehensive, rather than reviewing each individual Event. The review will determine if significant Events or exceptions have been handled appropriately. The review also tracks, trends, and counts Event types. When an Event triggers an Incident, Problem, or Change Record, the review will verify that the handoff between the Event Management process and other processes took place as designed.

INCIDENT MANAGEMENT

CenturyLink will provide an Incident Management Service to Customer, including a Critical Incident Management Service and Security Incident Management Service. Incident Management is the process for dealing with all Incidents. This can include failures, issues, or questions reported by Users, by technical staff, or automatically detected and reported by event monitoring tools.

The purpose of Incident Management Service is to restore normal service as quickly as possible, in order to minimize any adverse impact on business operations. Incidents are often detected by the Event Management Service, or by Users who contact the Service Desk. Incidents are categorized to identify who should work on them and for trend analysis. They are prioritized according to urgency and business impact.

(A) Incident Management Scope

The activities within the Incident Management process include:

- Incident detection and recording
- Classification and initial support
- Investigation and analysis
- Resolution and recovery
- Incident closure
- Incident ownership, monitoring, tracking and communication

(1) Critical Incident Management

The Critical Incident process is triggered when an incident is detected or reported that meets the criteria specified in Section 2.2.2 below for a Priority 1 incident. The criteria that characterize the occurrence of a major incident are one or more of the following:

- A critical business service (as defined by Customer) is unavailable or is severely degraded or experiencing complete loss of service
- Data storage is compromised or completely inaccessible
- Network components and Communication links are down, including backup link
- A serious security breach affecting integrating of the process & data
- Surveillance systems are down

The following are the activities CenturyLink will perform as part of the Critical Incident Management process:

- Facilitation of outage calls
- Initiation of outage-related communications
- Engagement of Rapid Response Teams (RRTs)
- Invocation of appropriate escalation process

(2) Incident Management Scope

The Security Incident process is triggered when an incident is detected or reported that meets the criteria specified in the Incident Management process for a Security incident. The criteria that characterize the occurrence of a Security incident are one or more of the following:

- Security Incident Management criteria will be defined by Customer pursuant to Customer's Security Policy and Process documentation.

The following are the activities CenturyLink will perform as part of the Security Incident Management process:

- Facilitation of security incident calls
- Initiation of security incident-related communications
- Engagement Rapid Response Teams (RRTs)
- Activation of appropriate lockdown process as defined in Customer's Security Policy and Process documentation
- Invocation of appropriate escalation process

(B) Incident Priority Levels

Incident Priority	Business Impact
P1 **(Critical)**	An Incident affecting: • A business-critical application (as defined by Customer and documented in the Service Operations Documentation) or a business-critical application that affects a high number of End Users (as defined by Customer and for which a delay in restoration of service is not acceptable (complete loss of service). • An outage directly impacting revenue because of total loss of functionality of a business-critical application. • A Security Incident at the request of an authorized agent of Customer. Customer will provide a list of authorized agents.
P2 **(High)**	• An Incident affecting a business-important application (as defined by Customer) or a high number of Users and for which a delay in restoration of service is not acceptable (as defined by Customer). • Very limited number of overall functionality available • Severely degraded performance for a majority of users • Non-P1 Security Incident as defined in the Service Operations Documentation • VIP Support, Customer will provide a list of VIP users.
P3 **(Medium)**	An Incident affecting normal (non-critical or important) applications and a limited number of Users (as defined by Customer).
P4 **(Low)**	An Incident with low or no visibility that has no direct impact on systems, customers, Users, or revenue (as defined by Customer).

PROBLEM MANAGEMENT

CenturyLink will provide Problem Management Service to Customer. Problem Management Service will minimize the adverse impact of Incidents and Problems on Customer's users and prevent the recurrence of Incidents. CenturyLink will employ a Problem Management methodology to identify root causes of problems and initiate actions to remediate the problematic condition.

Once a Problem is identified, efforts will be made to determine the root cause. Successful analysis of a root cause identifies a known error condition. Known Error Conditions trigger a Request for Change, which identifies a specific item that the Change Advisory Board (CAB) must evaluate and act upon.

The Problem Management can involve both reactive and proactive efforts.

- Reactive Response—Response to Incidents that have been raise by users and brought to the attention of Service Desk personnel
- Proactive Action—Actions are proactively taken to resolve problematic conditions prior to the occurrence of an Incident.

The activities that occur as part of the Problem Management process are the following.

- Problem Identification—Incidents that reoccur three (3) times within a rolling ninety (90) day period will be classified as a Problem. All P1 issues are automatically classified as a Problem.
- Problem Ticket Creation—Problem tickets are created and linked to the appropriate Incident tickets.
- Problem Assignment—Problem tickets are routed to the appropriate resolver group.
- Problem Analysis—Performance of Root Cause Analysis (RCA) for all Problems to identify underlying causes.
- Requests for Change—Based on the results of the RCA, CenturyLink will submit a SOW Change Request to the CAB, if necessary.
- Resolution Validation—CenturyLink will validate with Customer that a specific problem has been resolved.
- Ticket Closure—Closure of a specific Problem ticket and update the status of Incident tickets.

CONTROL OF SOW CHANGE REQUESTS

(A) Change Control Scope

Customer is limited to ten (10) Customer-initiated or planned SOW Change Requests each month, assuming a reasonably consistent distribution of workload throughout the month. If, following the first three (3) months after Commencement Date, the actual Customer SOW Change Request volumes exceed the monthly limit of 10 change requests by ten percent (10%), CenturyLink will require a signed SOW Change Request to adjust the fees and Service Level Agreements to support the higher SOW Change Request volume. Until such SOW Change Request is executed, CenturyLink will respond to change requests with commercially reasonable efforts, but the Service Level Calculation Exclusion will apply to the SLAs applicable to Change Control. CenturyLink shall not be limited in the number of CenturyLink initiated changes required in the performance of in-scope Services. There shall be no limit on either party on the number of preapproved standard changes. Standard changes will be mutually agreed-upon.

(B) Change Control Activities

CenturyLink will be responsible for the management of Changes that relate to Services being provided to Customer by CenturyLink. CenturyLink will follow standard processes and procedures to report, assess, track, and complete Changes. These standards, processes, and procedures will be documented and approved by Customer's authorized representatives during the transition of Services. CenturyLink will participate in Customer's Change Advisory Board (CAB) meetings.

CenturyLink will perform the following activities as part of the Change Management Process.

- Planning
  - Create a back out and recovery plan
  - Build the Change schedule
  - Create change completion criteria
  - Assess risk of the Change to the environment and recommend risk mitigation measures
    - Define process for Outages caused By Change (OBC)
  - Develop Change implementation plan
  - Develop back out plan (in case change is not successful or business wants to revert back to previous release)
- Approval
  - Create RFC
  - Seek approval from CAB
  - CAB must approve in writing or via email for emergency changes ONLY
- Implementation
  - Execution of the approve Change
  - Test and validation of the implemented change
  - User sign off
- Closure
  - Post Implementation Review (PIR)

Change: The alteration of an existing User Device or software application configuration in order that it may deliver desired functionality.

Change Management: The Process responsible for controlling the lifecycle of all Changes. The primary objective of Change Management is to enable beneficial Changes be made, with minimum disruption to IT Services.

Change Record: A record containing the details of a Change. Each Change Record documents the lifecycle of a single Change. A Change Record is created for every request for Change that is received even those that are subsequently rejected.

Change Request: A formal proposal for a Change to be made. A Change Request includes details of the proposed Change, and may be recorded on paper or electronically.

SERVICE REQUEST MANAGEMENT

CenturyLink will be responsible for Service Request Management. A Service Request is defined as a User request for assistance unrelated to an Incident or Problem. All Service Requests are captured and are tracked by the ITSM tool. Common Service Requests include but are not limited to:

- Password Resets
- New user on-boarding
- User termination
- Privilege and access requests
- Hard and soft install, move, add, and change (IMAC)

(A) Service Request Scope

CenturyLink will handle Service Requests across all in-scope Services, assuming a reasonably consistent distribution of workload over the course of each month.

(B) Service Request Categorization

Requests are categorized by their estimated time to complete. Estimated Completion Time is defined as the time within which CenturyLink can reasonably be expected to complete the requested task or activity. Categorization of Service Requests will be in the Service Operations documentation that will be created during Transition.

Request Category	Estimated Completion Time
R1	1 Calendar Day
R2	2 Business Days
R3	5 Business Days
R4 Uncategorized	TBD

AVAILABILTY MANAGEMENT

CenturyLink is responsible for Availability Management (AVM). With AVM, CenturyLink will define, analyze, plan, measure, and improve availability of in-scope Services. CenturyLink will ensure that all Services in scope, processes, tools and roles are appropriate to achieve Service Level Targets for Availability through the use of AVM.

CenturyLink will perform the following actions as part of Availability Management:

- Identify and define Availability requirements
- Evaluate the Availability procedures and measures
- Report on Availability and trends
- Suggest and, if requested, conduct Availability audit and improvement

CAPACITY MANAGEMENT

CenturyLink will provide Capacity Management to Customer. Capacity Management ensures that systems that carry service workloads are capable of meeting expected performance levels by identifying existing system capacity and identifying any performance degradation that could reasonably be expected to occur in the event that increased demands are place on the system.

The intent of Capacity Management is to proactively manage computing & other resources (agreed upon by CenturyLink) to avoid degradation in performance, operational excellence, and ultimately future outages by identifying resource gaps or capacity-add in advance.

CenturyLink will present a performance analysis of physical and virtual machines each month and performance trends during the previous six (6) months for the following.

- CPU utilization
- Memory utilization
- % of available disk space
- I/O for disk and network throughput/latency
- Concurrent and active Users
- Database growth

In addition, CenturyLink will be responsible for presenting recommendations regarding future capacity requirements

PERFORMANCE MANAGEMENT

CenturyLink will provide Performance Management Services to Customer. The Services will:

- Proactively monitor Customer infrastructure to identify root causes related to performance degradation
- Track trends for various key performance indicators to forecast potential performance issues and opportunities for improvement
- Make recommendations to address performance bottlenecks
- Implement mutually-approved remediation steps to address performance bottlenecks

ASSET MANAGEMENT

CenturyLink will provide IT Asset Management Service to Customer. The Services will:

- Track inventory of assets related to in-scope Services
- Include a configuration management database for tracking, managing and updating inventory
- Manage the asset lifecycle from planning to disposal
- Create standards and processes for managing assets

CenturyLink will not be responsible for the procurement, validation, and legality of licenses deployed on Customer's infrastructure.

ADDITIONAL ACTIVITIES

CenturyLink will be responsible for the following additional activities:

- Vendor ticket initiation and coordination
- Call list maintenance
- Management notifications
- Time keeper function
- Incident post mortems
- Reporting basic network performance to Customer, including:
  - throughput
  - availability
  - capacity

RESPONSIBILTY MATRIX

The responsibilities of CenturyLink and Customer associated with the delivery of Services are set forth below.

ITIL Service Desk	CenturyLink	Customer
Event Management		
Monitoring of in-scope components	✓	
Incident Management		
Logging of end user calls and work requests	✓	
Incident Support call resolution	✓	
Notification and escalation to higher levels of support	✓	
Reporting (daily/weekly/monthly)	✓	
Web interface to receive request	✓	
Knowledge base for end users to query	✓	
Call recording for evaluation	✓	
Escalations of Incidents	✓	
Automated ticket status changes to requesters	✓	
Incident closure	✓	
Problem Management		
Initiate root cause process	✓	
Perform root cause analysis and delivery report	✓	
Update knowledge base on finding of solution	✓	
Initiate Change Request to eliminate root cause	✓	

Problem closure	✓	
Configuration Management		
Maintain configuration baselines	✓	
Implement configuration and patching audits, verification and reporting	✓	
Change Management		
Initiate change request	✓	✓
Review and approve/reject RFC		✓
Participate in CAB meeting	✓	✓
Implement change	✓	
Verify change ticket	✓	✓
Update change ticket	✓	
Functional Testing & Production acceptance of change		✓
Close change ticket	✓	
Service Requests		
Receive requests for allocation or modification to the infrastructure and applications	✓	
Track requests and report status of the request to Customer	✓	
Interface with Configuration Management team to implement allocation or modification to the infrastructure and applications	✓	
Availability Management		
Implement tools to monitor and ensure Service Availability is being maintained	✓	
Proactively take corrective action ensure Availability targets are met	✓	
Provide reports measuring Availability	✓	
Performance Management		
Proactively monitor the infrastructure to identify root causes related to performance degradation	✓	
Trend various key performance indicators to forecast potential performance issues and opportunities	✓	
Make recommendations to address performance bottlenecks	✓	
Implement approved remediation steps to address performance bottlenecks	✓	
Asset Management		
Control inventory related to in-scope Services	✓	
Provide a configuration management database for tracking inventory	✓	
Manage the asset life cycle from planning to disposal	✓	
Create standards and processes for managing assets	✓	
Other activities		
Third-party ticket initiation & coordination (in-scope ONLY)	✓	
Knowledge Base Management	✓	
Maintain call list, management notifications, time keeper function, post mortems	✓	