# CENTURYLINK INFRASTRUCTURE & APPLICATION MANAGEMENT SERVICES
# SERVICE GUIDE FOR SECURITY ADMINISTRATION SERVICES

This Service Guide ("SG") sets forth a description of the Security Administration 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 and service description terms are set forth in this SG.

## SERVICE DESCRIPTION

CenturyLink will be responsible for providing Services by implementing and executing the Customer IT Corporate Security Policies which would include:

- Management and 24x7x365 monitoring of below mentioned Infrastructure and platform components within the Customer IT environment:
  - Network Routers and Switches
  - Firewalls (Physical and Virtual)
  - Servers
  - Desktops
  - Mobile devices
  - Storage (SAN, NAS)
  - Exchange
  - Active Directory
  - User ID Administration
  - Antivirus
  - Backup & Restore

- In addition to the infrastructure and platform components, CenturyLink will also provide coordination and access support for the following activities:
  - On-demand security and compliance reporting
  - Collection, archival, search and reporting of raw log data from security devices, network infrastructure, servers and other log sources
  - Security Audit
  - Third parties engaged by the Customer to provide Security Services
  - Security Incident Management

- CenturyLink will perform the following activities when implementing Customer's IT Corporate Security Policy:
  - Identity and Access Management
  - Authentication & Authorization policies
  - Antivirus
  - Email
  - Mobile Device Security
  - Firewall Rules
  - Back-up
  - Encryption
  - Audit Support

## RESPONSIBILITY MATRIX

The responsibilities of CenturyLink and Customer associated with the delivery of Services are set forth below. During the transition of Services, CenturyLink and Customer will agree on parameters to be monitored, associated thresholds, actions to be taken and reports to be produced. These parameters along with delivery processes and procedures will be documented in Customer's Service Operations Documentation.

| Responsibility – Security Administration Services | CenturyLink | Customer |
|---|---|---|
| **Design:** | | |

| Responsibility – Security Administration Services | CenturyLink | Customer |
|---|---|---|
| • Security Policies for Servers, Databases, Network etc. | | ✓ |
| • Security Policies to include provisions for Virus Protection at the Email, Server, desktop & notebook levels including automatic monitoring for viruses and automatic repair or deletion of infected files | | ✓ |
| • Security Reports | ✓ | |
| • Report on major viruses' outbreaks, detailing actions taken to resolve and prevent recurrence | ✓ | |
| **Approve:** | | |
| • Security roles and profiles | | ✓ |
| • Security related changes | | ✓ |
| **Implement:** | | |
| • Security Policies for Servers, Databases, Network etc. | ✓ | |
| • Security software upgrade and patch management | ✓ | |
| **Validate:** | | |
| • Security reports | | ✓ |
| • Security changes | | ✓ |
| • Audit reports | | ✓ |

The Customer IT Corporate Security Policy must include provisions for Virus Protection at the Email, Server, Desktop and mobile devices including automatic monitoring for viruses and automatic repair or deletion of infected files.