CenturyLink

Customer Information Guide & Handbook

Kathy Jones Repage
Director, Colocation Product Management
July 27, 2015
Document Revision 5.3

CenturyLink
www.centurylink.com

Town & Country, MO 63017
Office: 314.628.7000

Copyright 2015 CenturyLink Inc. All rights reserved.
CenturyLink ® is the registered trademark of CenturyLink Communications Corporation.
No part of this document may be reproduced, transmitted, distributed, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of CenturyLink.

The products described herein are CenturyLink's intellectual property and may be protected by one or more U.S. or foreign patents or pending patent applications.

Published in the United States of America

THIS DOCUMENTATION CONSTITUTES PROPRIETARY, CONFIDENTIAL INFORMATION OF CENTURYLINK, INC., AND MAY NOT BE DISCLOSED OR USED EXCEPT AS MAY BE PROVIDED IN THE TERMS AND CONDITIONS OF THE SERVICE AGREEMENT PURSUANT TO WHICH YOU HAVE BEEN AUTHORIZED TO USE THE PRODUCT OR TO REVIEW THIS DOCUMENT.

One or more of the following U.S. Patents may protect the technology described herein: 5,978,791, 6,185,598, 6,415,280, 6,275,470, and 6,130,890. Additional patents are pending worldwide.

CenturyLink, Inc.
1 Solutions Parkway
St. Louis, MO 63017
Toll-Free in USA: 800.728.8471
Outside USA: 314.628.7000

Table of Contents

Introduction

Welcome to CenturyLink. We are happy that you have become a CenturyLink customer and want you to know that we are committed to exceeding your expectations and are looking forward to developing a long and productive relationship.

The objective of this handbook is to provide you with sufficient information regarding the ongoing support of your CenturyLink Colocation services. This guide covers essential processes and policies such as our data center visitation process, security and operational policies, installation and maintenance guidelines, how to request new services and upgrades, incident reporting, problem escalations, and other items to ensure that the important aspects of your CenturyLink engagement are clear and straightforward.

SavvisStation Portal

In the fast-paced world of managing IT infrastructure it is critical to have the proper information at your fingertips. Whether it is bandwidth reports, case management, or change management status, up-to-date information is critical to making the right business decisions. Having access to critical information needs to be simple and intuitive. The information also needs to be presented in an informative manner. To help customers meet these needs CenturyLink has created the SavvisStation Portal.

The Portal is a web-based view of your CenturyLink products and services via a standard Internet browser. It provides a set of reports and interactive information on the services received. CenturyLink customers manage their own access to the SavvisStation Portal. User access is controlled through three types of accounts: admin, read/write, and read-only. Separate permissions can also be given to users needing to view Invoices and Security information.

Through the SavvisStation Portal you can update your company's contact list from any location with Internet access, conveniently and easily, and with immediate results.

The Portal helps manage the security of your company's contact list by controlling the appointment of Contact Administrators. Only Contact Administrators are able to update a company's contact list via eService. Furthermore, CenturyLink's Service Desk staff only accepts contact update requests from your designated Contact Administrators.

Customers have complete access control of their contact list and can rapidly deactivate contacts if circumstances require, such as an employee departing the company. To access the contact management tool, you simply need to login to the portal at http://www.savvisstation.com using your assigned userid and password. Once logged in to the portal, click on the *Support* header tab, then *settings tab*, choose *admin settings* then choose *contact administration*.

The portal provides a wealth of vital information including monitoring of physical inventory, real-time and historical statistics on server resource utilization, bandwidth utilization statistics, real-time status of trouble tickets, billing invoices, Gold Support metrics and status of open orders. You can also create new cases, create and manage change requests, request for service disconnects, create and manage contacts as well

as login via the portal.

In addition, you can view a range of statistics related to access circuits, server memory, disk, and processor usage. This data can be viewed on a daily, weekly, monthly, quarterly and yearly basis, providing you with critical information needed to assess the performance of each server, network, connection, and website.

Your CenturyLink account team can provide you with a SavvisStation Portal User Guide and temporary password to view a tutorial of the system, which is available at http://www.savvisstation.com. To obtain an account, please call the CenturyLink Service Desk or email ColoSupport@Centurylink.com. For existing SavvisStation Portal accounts, the User Guide is available on the web portal, which is accessible to you on a 24/7 basis. Your account team and/or the Service Desk can set up your company with user accounts.

Gold Support

Gold Support Service provides Network and Systems remote or on-site ("hands-on") support for our customers' environments within CenturyLink's data centers. Gold Support is purchased in three forms: prepaid block of hours or ad hoc.

- Prepaid Gold Support-Monthly Recurring Option is for a fixed block of support hours purchased each month. Support hours provided at Customer's request during a calendar month are subtracted from the number of hours purchased. Unused hours may not be carried into successive months. Customer shall remit payment for all hours billed regardless of whether hours are used.
- Prepaid Gold Support-Non Recurring Option is for a fixed block of support hours purchased and consumed over several months. Support hours provided at Customer's request are subtracted from the number of hours purchased until exhausted.
- No Commitment or Ad hoc Gold Support is purchased for those instances where there are unplanned events and are not purchased in advance.

Each plan provides 24/7 support by CenturyLink Support Engineers and is billed in 15 minute increments. To request Gold Support services you may do so by opening a ticket in SavvisStation.

CenturyLink Facility Infrastructure Overview

Infrastructure Maintenance – Approval Process and Schedule

CenturyLink schedules routine maintenance to enable work to be performed that improves the CenturyLink network and facility infrastructures. Additionally, preventative maintenance is performed to remedy potential events that have been identified by CenturyLink's early warning procedures and processes. These potential events are derived by careful monitoring and thorough analysis of activity logs for our network and facilities.

All changes to the network and facilities are subject to CenturyLink's change management process. During the process that work is reviewed for completeness (risk assessment, completed test procedure, metrics for measuring progress, back out procedure, etc.) and accuracy prior to scheduling and implementation.

The goals of change management are:

- Implement changes to CenturyLink services, infrastructure, policies and procedures in an effective and efficient manner;
- Minimize risk and impact to our customers;
- Enable CenturyLink to be proactive in notifying you of potential disruptions to service;
- Test all new equipment or routing configurations using CenturyLink's independent test network prior to deployment as part of the data center configuration.

CenturyLink strives to prevent disruptions in service and targets to perform maintenance during low traffic times in order to minimize potential interruptions to your operations.

Planned Maintenance Schedule – Saturday	
All published times are local to the region in which the maintenance is being executed unless otherwise noted.	
United States, South America	
Local Time	12:00 am – 5:00 am
Canada	Sat & Sun 00:00 (midnight) to 08:00am EST
Local Time	12:00 am – 08:00 am
Continental Europe and South Africa	
Local Time	12:00 am – 4:00 am
Asia Pacific	

GMT	9:00 pm – 1:00 am Sunday
Planned Maintenance Schedule – Sunday	
United States, South America	
Local Time	12:00 am – 5:00 am
Japan	
Local Time	4:00 am – 8:00 am
Canada	
Local time	Sat & Sun 00:00 (midnight) to 08:00am EST
Planned Maintenance Schedule - Wednesday	
Canada	
Local time	Wed 01:00-05:00am EST

Weekly Maintenance Notifications

Weekly maintenance notifications are only issued to contacts that have been identified as "Technical Notification Contacts".

The Weekly Maintenance Notification informs you of any local or global improvements to CenturyLink Technology Solutions' network or infrastructure. In most instances, the Weekly Maintenance Notification will be issued 10 days prior to the scheduled work, with the exception of emergency maintenance actions, which will be handled as needed.

If a mission critical situation arises, CenturyLink will promptly contact you by using its Emergency Contact Procedures. Only Technical Notification Contacts with e-mail addresses and text pagers on file with CenturyLink will be notified in the event of a network or facilities event involving multiple customers. An alert e-mail will also be sent to notify all affected customers with details of the event. Periodic updates throughout the course of the incident will be provided.

All maintenance notifications are available on the SavvisStation portal at http://www.savvisstation.com. Visit the SavvisStation website on Wednesdays for the most recent maintenance information. Each posting will provide notice of upcoming scheduled maintenance. Emergency maintenance may not be posted because of its immediate nature. The anticipated duration of outage will vary by city. Please refer to the individual tickets listed on the website.

CenturyLink strives to keep you informed of changes and maintenance. If you are ever in doubt as to whether a particular maintenance will affect (or has affected) your company, please call or e-mail the Service Desk with the Activity number and ask that a case be opened and/or escalated to determine the

extent of impact. If you are not receiving maintenance notifications, please call the CenturyLink Service Desk at 888-638-6771 or send an email to request@savvis.net.

Data Center Power Specifications

All CenturyLink data centers provide uninterruptible power in-line with UPS and diesel generator backup in the event of a utility power failure. To conform to the National Electrical Code (NEC) for maximum power use, each power circuit is limited to 80% of the circuit breaker rating. In addition, Customer's total power consumption associated with its Services shall not exceed the Committed Electrical Capacity (CEC) as stated on your Service order. All data centers have minimum watts per square foot ratings as set forth in the table below.

Data Center	Data Center Location	Minimum Watts sq./ft.
AT1	Atlanta, GA	165
AB3	Albuquerque, NM (Floor 3)	150
AB3	Albuquerque, NM (Floor 4)	150
BO1	Boston, MA	150
BO2	Boston, MA	150
BO3	Boston, MA	150
BR1	Burbank, CA	150
CH2	Chicago, IL	150
CH3	Chicago, IL	150
CH4	Chicago, IL (Suite 410)	163
CH4	Chicago, IL (Suite 810)	200
CH4	Chicago, IL (Suite 830)	200
CL1	North Lewis Center, OH	150
CW1	Moses Lake, WA	150
DC2	Sterling, VA	150
DC3	Sterling, VA	150
DC4	Sterling, VA	150
DC5	Sterling, VA	150
DC6	Sterling, VA	150
DC7	Sterling, VA	150
DL1	Dallas, TX	150
DL2	Dallas, TX	170
DN1	Highlands Ranch, CO	150
DN2	Highlands Ranch, CO	200
DN3	Englewood, CO	150
LA1	El Segundo, CA	150
LV8	Las Vegas, NV	175
LV9	Las Vegas, NV	175
MP1	Minneapolis, MN	150
MP2	Shakopee, MN	150
NJ1	Jersey City, NJ	150
NJ2	Weehawken, NJ	150
NJ2	Weehawken, NJ (Suite 130)	150

Data Center	Data Center Location	Minimum Watts sq./ft.
NJ2X	Weehawken, NJ	175
NJ3	Piscataway, NJ	150
NJ4	Piscataway, NJ	150
NJ5	Newark, NJ	150
OC2	Irvine, CA	150
PH1	Scottsdale, AZ	150
PH2	Phoenix, AZ	150
SC4	Santa Clara, CA	150
SC5	Santa Clara, CA	150
SC8	Santa Clara, CA	150
SC9	Santa Clara, CA	150
SE2	Seattle, WA	150
SE3	Seattle, WA	150
SE4	Tukwila, WA	150
SL1	Hazelwood, MO	150
SN1	Sunnyvale, CA	150
SN2	Sunnyvale, CA	150
TP1	Tampa, FL	150
Canada		
MR1	Montreal, Quebec	150
TR1	Mississauga, Ontario	150
TR3	Markham, Ontario	150
VC1	Vancouver BC	150
EMEA		
FR6	Frankfurt, DE	150
LO1	Slough, UK	150
LO3	London, UK	150
LO4	London, UK	150
LO5	Slough, UK	150
LO6	Winnerish, UK	150
Asia		
3PBRIS1	Brisbane	150
3PCANB1	Canberra	150
3PMELB1	Melbourne	150
3PPER1	Perth	150
3PSY4	Sydney	150
HK2	Hong Kong	150
SG2	Jurong East, SG	150
SG8	Geo-Tele Centre, SG	150
TY6	Tokyo, Japan	150

If CenturyLink reasonably believes that Customer power usage exceeds the Permitted Power Usage, CenturyLink reserves the right to require that Customer order a periodic power audit to ensure Customer's compliance with the Permitted Power Usage, which such audit will be performed by CenturyLink at contracted time and materials charges. Power audits will be performed as Gold Support hours and charged as such. If CenturyLink determines that Customer's actual power consumption exceeds the Permitted Power Usage, CenturyLink shall so notify Customer and Customer shall:

a) Reimburse CenturyLink the cost of such power audit as invoiced by CenturyLink, and
b) Have five (5) days to commence remedial action to comply with the Permitted Power Usage.

Such remedial steps may include, but are not limited to, Customer decreasing the amount of its power usage and/or purchasing additional sufficient space or power in order to bring the environment in to compliance with the Permitted Power Usage.

If Customer fails to take appropriate remedial action within 5 business days of CenturyLink's determination, CenturyLink may

a) Suspend service without any further notification Service until such time as CenturyLink determines that Customer's power consumption complies with the Permitted Power Usage, and/or
b) Terminate the applicable Service upon five (5) days' notice.

Customer installation shall be consistent with CenturyLink's requirement that customers distribute power evenly among all available power circuits. Care should be taken that you consider your future expansion plans and how this may affect your power distribution. If you do not plan this carefully from the beginning, you may exceed your power requirements on a particular circuit and you may need to power down some of your equipment in order to return your power configuration to a CenturyLink approved load.

For liability purposes CenturyLink does not provide any power cables for customer equipment. Daisy chaining of power strips or the use of extension cords of any type is **STRICTLY PROHIBITED**. When an additional outlet is needed, you must purchase additional power circuits. Alternatively, if your existing power circuit can bear additional load and you are not exceeding permitted power usage, you may purchase a power strip with additional outlets. Customer provided power strips must be the metered display type and installed by CenturyLink.

Additional power terms are documented in the CenturyLink Colocation SSG.

Specific to the Las Vegas Data Centers

In order to maximize the efficiency of the data center space, Customer must run equipment power cables as follows:

- Zip-tie power cables underneath Customer's corresponding ladder rack and run cables down and behind all ladder racking.
- Customer shall not run power cables down the front of the ladder racking or zip-tie them to the outside of the racks.

- Ten to fifteen foot cords are recommended as PDU and or ATS cords need to be long enough to reach the power receptacles.

Hot and Cold Aisle Compliance

Customer must receive approval from CenturyLink with regards to hot and cold aisle layout configuration and adhere to those requirements prior to equipment installation.

Special venting configurations must be pre-approved by CenturyLink and will incur additional Customer set-up costs.

All computerized equipment generates heat. All equipment placed in any data center must vent the heat directly into the hot aisle where it is then contained and prevented from mixing back into the cold aisle.

Customer must close any void in cabinet or rack space with a blanking panel. Periodic compliance audits will be conducted and Customer will be notified of blanking panel management violations and are required to close any rack void with a blanking panel within five (5) business days of notification. If five business days have passed and the void in the rack or cabinet has not been closed, CenturyLink will perform this duty at the Gold Support rate.

Physical Security

The Global data center Security and the Physical Security organizations within CenturyLink Corporate Security have global responsibility for all physical security operations, security systems, access administration, and security controls within CenturyLink data centers.

CenturyLink Corporate Security has implemented Security Policies to reinforce the importance of physical security of all data centers including policies and procedures specific to data center physical security. Policies are reviewed annually, or as needed for relevance and amended to reflect changes in requirements, technology and other circumstances. Internal audits may be carried out to enforce the Policies and Procedures and if any violations are discovered the appropriate disciplinary action is taken, up to and including termination of employment.

Global Data Center Security operation is a multidisciplinary organization that combines security and data center operations expertise. Data Center Security personnel receive security training and certification prior to their full-time assignment within a data center and continuously thereafter. Data Center Security personnel also maintain First Aid, CPR and AED training certifications.

Each data center has a Security Operations Center (SOC) or security desk. Data Center Security personnel control data center access, monitor security alarms and closed-circuit television (CCTV) cameras, and manage all security-related issues from the SOC or security desk.

The Corporate Security Operations Center (CSOC) provides global, 24/7 support to the local data center security teams with remote monitoring, management, administration and maintenance of the access control systems and Closed Circuit Television (CCTV) video surveillance systems used throughout CenturyLink data centers. The CSOC also assists and directs local data center security in the response to critical alarms, physical security incidents and critical events involving law enforcement, fire or emergency medical personnel.

The Central Access Control Center (CACC) within CenturyLink Corporate Security supports the distribution of all CTS access badges and the administration of access permissions within the access control system.

Specific to the Phoenix Data Centers

In the PH1 (Phoenix) data center badging hours are Monday and Thursday between 1-4 PM and PH2 (Scottsdale) badging hours are by appointment.

Specific to the Australia Data Centers

Any individual permitted access to an Australia data center is required to undertake an induction prior to being able to access the facility unescorted. A separate site induction is required for each of the Australia facilities. Inductions are valid for 12 months after which the individual is required to attend a refresher induction if continued access is required. Please place a ticket via the SavvisStation portal to make arrangements for your induction.

Confidentiality

CenturyLink respects the confidentiality of our customers and works toward anonymity for all data centers to reduce security risks. CenturyLink considers the street address and location of its data centers to be confidential information to our business which is made available to our customers and suppliers under Non-Disclosure Agreements. CenturyLink customers and contractors should not use social media in any way that may divulge the data center location, physical address or any information that is confidential, proprietary or has not otherwise been made public by CenturyLink.

Signage

For aesthetic, privacy and security reasons the posting of signage is prohibited by customers and contractors inside the data center.

Access to the Data Center

Normal data center hours are 8:00 a.m. to 5:00 p.m. local time, Monday through Friday.

Customers and their authorized representatives can access the data center and their colocation space on a 24/7 basis. Individuals granted permanent or temporary access will have unescorted access to the assigned colocation space dependent upon local conditions.

Minors, 16 years of age and younger and not a Customer employee, must have a legitimate business need and prior authorization from data center management to be granted access to the secured data center colocation areas.

For customers in certain data centers, including Hazelwood SL1 (US), Minneapolis MP1 (US), Phoenix PH1 (US), Scottsdale PH2 (US), Montreal MR1 (CA), and Docklands LO4 (UK), a ticket must be opened 24 hours prior to arrival to alert staff of the impending visit.

All persons are to enter and exit the data center through the authorized main entrances only. Customers and their authorized representatives are not to enter or exit the data center through the loading dock and service exits. Emergency exits are to be used only in the case of a Fire or Life Safety emergency.

CenturyLink utilizes mantrap portals combined with a two-factor authentication of each individual entering the data center front entrance to control access to the data center and prevent tailgating, defined as the practice of one individual entering the data center or colocation area by following behind another individual with badge access. The two-factor authentication involves granting a person access based upon a combination of presenting a valid CenturyLink access badge and a verification of the badge holder using a biometric (hand or finger) scan or Personal Identification Number (PIN) code. Two-factor authentication is always required to enter the secured, raised floor colocation areas of the data center.

All persons requesting access to a CenturyLink data center must verify their identity by presenting valid government-issued photo identification or a Savvis-issued photo access badge. Examples of valid government-issued photo identification include a passport, driver's license, military IDs, State identification

card, etc.

Security Specific to the Las Vegas Sites

In the Las Vegas site(s) you must call security using the provided intercom at the door. You must use your access card at the exterior reader. Upon entry, security will verify card holder identity using the data center access control system. After all persons in the man-trap are identified, Security will initiate the turnstile biometric reader for use. All persons, including guests must use Switch issued badges when entering any area. Badges must be worn on the issued colored lanyard and visible at all times while in the facility. You may not lend your access control badge to another or wear a Switch photo identification badge in public. Regardless of your geographical location, if your security badge becomes lost or stolen, contact security immediately.

Entry and Exit Inspections

CenturyLink reserves the right to inspect any and all incoming or outgoing property. Additionally, Savvis reserves the right to inspect any and all containers/items in the possession of any individual at any time while on CenturyLink property.

Access Control Systems and Badges

CenturyLink uses an access control system (ACS) and access badges to restrict access within data centers to only those individuals with proper authorization. In all data centers except Hazelwood, MO, Phoenix and Scottsdale, AZ, Frankfurt, Germany, Las Vegas, NV, Brisbane, Canberra, Perth, Sydney, and Melbourne, Australia, where a third-party ACS is used, CenturyLink owns, monitors and administers the ACS.

All persons entering the secured area of the data center are required to have a CenturyLink permanent, temporary or visitor access badge. Access badges are to be worn by the individual at, or above, the waist and be visible at all times. All access badges are the property of CenturyLink and must be returned upon request. No modifications or additions should be made that interfere with the visibility, clarity, or use of the badge.

CenturyLink access badges are issued to authorized individuals and are for their sole use only. The sharing of badges or PIN codes between individuals for any purpose whatsoever is strictly prohibited.

Customer is responsible for endorsing their employees and contractors access to the data center. This can be accomplished by placing a security ticket request in the SavvisStation portal. Customer badges remain active until the badge holder's authorization is revoked by the Customer. CenturyLink may, at its discretion and at any time, revoke the access privileges of any Customer badge holder as a corrective measure to security violations, inappropriate behavior, non-payment of account or other instances deemed appropriate by CenturyLink.

In the event a customer discontinues their colocation services with CenturyLink, all badge access privileges to CenturyLink Technology Services data center(s) will cease with the requested Stop Bill Date for such services.

Customer badges will be made inoperable if the not used for more than ninety (90) consecutive days. The badge holder may request re-activation of their badge on their next visit to the data center. Any badges which remain inoperable and unused for twelve (12) consecutive months will become completely inactive and require replacement.

Temporary badges are reserved for use by active CenturyLink access badge holders who have forgotten their badge or authorized individuals that only require temporary access. Any permanent access badge holder who has forgotten their badge should obtain a Temporary access badge from Data Center Security.

Temporary or Visitor access badges are valid only for the day and time specified. All individuals assigned Temporary or Visitor Badges are required to return the badges to data center security or deposit them in the Key and Badge Drop Box (where available) when departing the data center.

Customers and their authorized representatives may not enter the Managed Service, Node, and Meet Me Room areas of the data center at any time.

Access Control Specific to the Hazelwood, Missouri Data Center

The hours of operation in the Hazelwood data center are 8AM to 5PM central Monday through Friday. Access to the Hazelwood, Missouri data center outside of the hours of operation requires that the customer open a ticket via the customer portal at least 24 hours in advance of time of entry. Ticket requests posted after 5PM Central will be worked the following business day.

Access Control Specific to the Las Vegas Data Centers

Customers requiring access to the Switch data centers will be granted two access badges per contract. Additional badges will be provided for an additional fee. Customer employee's access will be granted only in the areas in fulfillment of their contracts. Customers who contract another person or company to be their representative and perform under contract within a Switch facility will be treated by Switch as an employee of the Customer. This includes protection by the Customer's insurance, workers compensation and other legal assurances to claims, holding Switch and its employees harmless.

The Customer's contractual point of contact identifies, in writing or email, a security point of contact for the Customer. The security point of contact is the only person who can request access for Customer employees at the site. The access notification must precede the person being granted access visit to the site and may not be brought to the site with that person. Customer employees will be photographed and one or more fingerprints will be recorded in Switch's access control system.

Access badges issued by Switch are the property of Switch. Upon Switch's request at any time, or upon termination of employment, contractor status, or customer contact, Customer will promptly return the Switch issued badge to the Switch Security Director.

Semi-annually, during March and September, or for cause, security will forward information to management and customer's security point of contact to review those having access, their access level and access rights. Continued access will be based upon the affirmative response by the security point of contact.

Data Center Cage and Cabinet Security Controls

All CenturyLink customer cages and cabinets come standard with either a metal lock with key or combination code. You may sign out keys and obtain combination codes as needed from Data Center Security.

You are not permitted to alter, change, or install any locking mechanism on your space. Additionally, you are not permitted to alter or change any CenturyLink owned cabinet or rack. This includes, but is not limited to, removal of doors, drilling holes or mounting equipment to the exterior of the cabinet or rack.

For an additional fee, CenturyLink will install, manage, and maintain proximity and/or biometric readers on your colocation space to replace the need for keys and/or combinations. Only CenturyLink approved and authorized security measures using the CenturyLink access control system may be installed in, or on, a Customer colocation space. Customers may engage their CenturyLink Account Manager to request CenturyLink electronic access control measures for their colocation environment. CenturyLink does not allow the installation of customer-owned security access control systems in the data center. This is necessary to preserve our compliance with various industry standards and ensure CenturyLink operations personnel and first responders have unimpeded, expeditious access to all colocation areas and occupants in life/safety emergency situations. CenturyLink retains all necessary rights to respond to any emergency with respect to Customer equipment in the data center.

Customers are not allowed to install their own security surveillance systems without prior approval from CenturyLink. (See Video Surveillance)

Metal Key Administration

Data Center Security maintains a minimum of two keys for each customer space, one back-up and one loaner. All metal keys are secured within the Security Operations Center (SOC). The back-up key is maintained by Data Center Security at all times in the event that an escort is needed to allow access to a customer's cage. Customers will not have possession of this back-up key at any time.

The loaner key will be available from Data Center Security for use in accessing your colocation cage. Persons authorized by you for permanent or temporary data center access may be issued a loaner key. The loaner key is issued to you for your use each day you visit the data center. A loaner key is not required if you have access control card or biometric readers already installed on your cage doors.

The person assigned the loaner key is responsible for returning the key to Data Center Security or in the Key and Badge Drop Box, where available, when departing the data center. Any loaner key that is reported as having left the data center premises is considered lost and will result in the customer colocation

space being secured with a chain and padlock by Data Center Security. The colocation space will be re-keyed within three (3) business days. You may be charged for the cost of the re-key. Access to your space while it is padlocked will be available by escort only.

Customer Metal Key Administrator

(Excludes Hazelwood and the London Data Centers)

As a colocation Customer, you have the option of managing your metal key. You must appoint a "Key Administrator" who is authorized to receive the metal key on your behalf. Your Key Administrator must be identified as such in your contact database. Your CenturyLink Account Representative can assist you in establishing your Key Administrator. CenturyLink data center Security will permanently issue your metal key to your Key Administrator. Once issued, it is the sole responsibility of the Customer Key Administrator, and not CenturyLink CenturyLink, to manage ownership, distribution, possession, and use of the key. Customer Key Administrators may make as many copies of the key as needed. By agreeing to administer your key, you acknowledge and accept that any person with a valid CenturyLink CenturyLink access badge and key has unrestricted access to your colocation space and CenturyLink is not responsible for any unauthorized access to your space.

Data Center Security will continue to have a loaner key be available for you in the event that you forgot a key or need to a key issued on a temporary basis.

Customer Access Authorization List

Customers are responsible to provide CenturyLink with, and maintain, an accurate listing of their employees, contactors and vendors requiring access into the CenturyLink data center and their colocation space. The Customer maintains their current access authorization list within the Contact Administration section of their Site Record in the CenturyLink Portal. Customers have control of, and are responsible for their access authorization list and can rapidly add or deactivate contacts as circumstances require.

Persons designated by the Customer as a "Contact Administrator" with administrative level permissions within the CenturyLink SavvisStation Portal, may add, change or delete active Contact records and add, change or remove access authorizations to an Active Contact record. The CenturyLink Service Desk and/or your CenturyLink Account Representatives have the authority to make changes to the contact information in the database upon request. In order to process any personnel changes that affect your contact list, you must contact CenturyLink CenturyLink in writing prior to revising access privileges in the access database. Contact the CenturyLink Service Desk to make the appropriate updates to the contact list in the database in the event the Account Representative cannot.

Data Center Security relies on your customer contact list in the database to verify access authorizations prior to granting access to the data center. All individuals who come to the data center to work on your behalf must also be listed in the database as an "active" Contact and be assigned data center access permissions to be granted entry to the data center and to your space. The Contact first and last name

should match their name as it appears on their government-issued photo identification.

Access authorization may be granted on a permanent or temporary basis to any active Contact on your account. Permanent access requires a Start Date and remains in effect until revoked by the Customer. Permanent access is recommended for persons requiring frequent access to your colocation area over a long, sustained period of time. Temporary access requires a Start Date and End Date and remains in effect during the time period specified. Temporary access is recommended for persons needing access during a short, specified period of time with known start and end dates.

Persons requiring access to more than one data center must have multiple instances of data center access permission, one for each data center, assigned to their Contact record.

Your Contact Administrator may also revoke access authorizations at any time by removing data center access permissions from an active Contact or simply making the Contact inactive.

All badge access privileges to CenturyLink data center(s) will cease with their Stop Bill Date for such services.

Customer Badge Issuance

CenturyLink Customer badge issuance is authorized by the Customer. Customer authorization is considered granted when the applicant is an active Contact under the Customer site record with permanent data center access permissions for the specified data center.

Only persons with permanent data center access permissions are eligible to be issued a CenturyLink Technology Services Customer badge. Persons with temporary data center access permissions are not eligible for a CenturyLink Customer badge and are provided a CenturyLink Temporary Customer badge while in the data center.

Customer badges are issued upon request. Individuals with permanent data center access permission may request a CenturyLink Customer badge by:

- Submitting an online request using the Badge Request form found on the CenturyLink Technology Services Station Portal within the Case Creation section under Colocation/Data Center Access; or
- Completing a badge request form in person with Data Center Security.

Security officers may create and provide the Customer with their Customer badge based upon the customer authorization. For audit purposes, an approved badge request must be submitted and approved within CenturyLink for each new badge issued.

CenturyLink customer badges are issued by Data Center Security during normal business hours. Before issuance of a CenturyLink Technology Solution Customer badge, the badge holder must verify their identity with their unexpired Government-issued photo identification. Customer badge issuance will require the badge holder to be photographed and complete a biometric enrollment using a hand or finger scan.

The CenturyLink Customer badge is intended solely for use by the individual identified on the badge and

may not be shared with or used by other persons.

Customers must display their CenturyLink Customer badge on and above their waist at all times while in the CenturyLink data center.

Persons, who have forgotten their CenturyLink Customer badge, may be provided a Temporary Customer badge.

Customer Access

CenturyLink Customers and their authorized representatives can access the data center and their colocation space on a 24/7 basis. Individuals granted permanent or temporary access will have unescorted access to the assigned colocation space dependent upon local conditions.

If you contract with third party technicians, they are held to the same requirements as your employees for gaining access to our data centers. You are responsible for their actions within the data center and ensuring their compliance with the terms of your service agreement and the CenturyLink acceptable use policy. Third party technicians who are listed as active Contacts with permanent or temporary access permissions in the database will be allowed access to your space.

Customers and their authorized representatives may only access those portions of the data center made available by CenturyLink to Customers for the placement of their equipment and use of the data center services (the "Customer Area"), and common areas of the data center (e.g., entryways and bathrooms) unless otherwise approved and accompanied by an authorized CenturyLink representative.

The following additional provisions shall apply to Customers and their authorized representatives when accessing a CenturyLink data center. Customers and their authorized representatives shall not:

- Allow any unauthorized persons to access the data center (e.g., by "tailgating" or other means),
- Use, touch, inspect or otherwise interface with any CenturyLink or third party property or equipment,
- Harass or interfere with the activities of any individual within the data center, including any employees or representatives of CenturyLink or other customers,
- Engage in any activity that is in violation of law or the CenturyLink Acceptable Use Policy.
- Store any computer hardware or other equipment in the Customer Area that is not required for the use or implementation of Services,
- Make any construction changes or alterations to the interior or exterior of the data center or the Customer Area,
- The above provisions are in addition to the rules of the individual data center policies or other CenturyLink security related policies.

Security Access Reports

Security Access Reports requested by the customer for audit purposes are fee based and issued to the customer Account Manager or Client Solutions. The timeframe for these types of requests is generally 7-10

business days. Electronic access reports for data center or cage access are available for ninety (90) days then archived. Customers may request access reports via the SavvisStation portal and by choosing data center Security Access Reports from the menu. Gold Support fees will be assessed for the assembling of these reports.

Visitor Access

A person entering a CenturyLink data center, who is not an authorized customer, employee, or contractor will be considered a Visitor and must demonstrate a legitimate business purpose for visiting the site. The Visitor must be escorted by an Authorized Sponsor at all times. Authorized Sponsors are CenturyLink employees or customers who have a permanent CenturyLink access badge and current access authorization to the data center. Authorized Sponsors are permitted to escort up to five Visitors at one time. Groups of six or more Visitors must be processed as a data center group tour. Contractors and third-party vendors are not permitted to sponsor Visitors.

All Visitors must:

- Sign-in with data center security with their Authorized Sponsor upon entering the data center.
- Verify their identity with valid (unexpired) government-issued photo identification.
- Receive a Visitor badge which must be visibly worn at, or above, the waist while in the data center
- Remain with their Authorized Sponsor at all times while in the data center.
- Sign-out with data center security and return the Visitor badge at the end of their visit.

All Authorized Sponsors must:

- Maintain visual contact with visitors at all times while on the data center premises.
- Ensure visitors wear and display a Visitor badge at all times
- Escort visitors to data center security at the end of their visit.
- Ensure visitors sign-out with data center security and return their Visitor badge.
- Remain responsible for visitors and not switch Authorized Sponsors without first signing-out the visitors with data center security. The new Authorized Sponsor must then sign-in visitors with data center security.

Data Center Tours

Data center tours are coordinated by your CenturyLink Account Team. Any company requesting a tour must have a Non-Disclosure Agreement (NDA) on file with CenturyLink. It is important to schedule your tour with as much lead time as possible and ensure that NDAs have been properly executed. Data center tours require the approval of data center management. Tour approval must be received at least three (3) business days in advance of the date the tour is to occur. All tours are conducted by the CenturyLink data

center management team. Gold Support fees will be assessed for any tours that are given at the request of the Customer. Tours should not exceed a 10:1 ratio of visitors to sponsor. To expedite visitor processing, Data Center Security should be provided the first and last name of all attendees at least one business day prior to the actual tour. The attendee first and last name should match their name as it appears on their government-issued photo identification. Attendees will be required to verify their identity by presenting a valid government-issued photo identification prior to accessing the data center.

The tour sponsor is responsible for the actions and safety of the visitors while they are in the CenturyLink data center.

Video Surveillance

CenturyLink data center premises are under 24 hour Closed Circuit Television (CCTV) video surveillance. CenturyLink CCTV systems are designed to cover the exterior and common interior spaces of the data center. Customer colocations space is not included within CenturyLink CCTV surveillance. All CenturyLink CCTV systems are designed to provide ninety (90) days of video retention.

Audio recording within CenturyLink data centers is prohibited.

Customers may provide and install video surveillance equipment within their colocation space. Customer video surveillance systems must be approved by CenturyLink prior to installation. All Customer video surveillance systems must comply with the following provisions (which are subject to change from time to time at CenturyLink' sole discretion).

- Customer may supply its own cameras, mounting kits and installation services or purchase them directly from CenturyLink.
- Customer owned surveillance systems will not be interconnected with CenturyLink surveillance systems.
- All third-party contractors used by the Customer to install their CCTV system must adhere to CenturyLink data center Work Rules as outlined in the data center work rules section of this document.
- Customers, or their contractors, may not lift the data center floor tiles or enter into the plenum above the cage for any reason.

All cameras and associated cabling installed by the Customer within their colocation space:

- Must be securely installed to assure that they do not present a safety issue. (Falling, head injuries, etc.)
- May not extend below the data center floor tiles or into the plenum above the cage.
- May not block any CenturyLink surveillance equipment.
- May not interfere with cage or cabinet access.
- Must have a fixed camera view feature limited so the maximum field of view includes only the customer's cabinets in the cage in which the cabinets are located. No cameras that are pan tilt, or zoom enabled may be installed.

- May not include audio recording.
- May not view outside the Customer cage into other cages or other areas of the data center.

After installation, the Customer must demonstrate to CenturyLink data center Facilities Management and Data Center Security their camera installation meets the above requirements. CenturyLink Technology Solutions reserves the right to periodically perform unannounced inspections of the surveillance equipment to ensure continued compliance with the above requirements. CenturyLink will notify the Customer of any non-compliance issues found. Customer shall remedy all non-compliance issues no more than three (3) business days following notice. If Customer fails to remedy such non-compliance within that period, CenturyLink reserves the right to disconnect any non-conforming camera.

CenturyLink will not monitor, nor respond to Customer owned video surveillance equipment alarms. Customer requests for assistance in responding to Customer-owned video surveillance systems alarms will be assessed and billed at the applicable Gold Support billing rates.

Photography Policy

CenturyLink does not authorize the photography, or image capture, of the interior or exterior of any CenturyLink data center facility without prior written authorization.

This policy applies to all image-capturing devices with either traditional or digital imaging capabilities. This includes all cameras (digital or film), all video recording devices (camcorders) and any other devices capable of capturing images including, but not limited to laptop computers, webcams, cellular phones, Smartphones, Tablets, and wearable devices such as Google Glass or GoPro.

Video with audio recording capabilities within a CenturyLink data center is strictly prohibited.

Customer requests to photograph, or image capture, their colocation space for internal purposes must demonstrate a specific business need which cannot be met without the taking of video or photographic images, and have prior written approval by the CenturyLink data center Facilities manager. Customer requests to photograph for marketing, or any other purpose, or photography to be conducted by a third party must have prior written approval by the relevant CenturyLink Data Center Facilities or Operations manager and CenturyLink Corporate Security.

Any persons engaged in unauthorized photography at a data center will be reported to Data Center Security immediately for intervention and all photographic records will be required to be destroyed or deleted. Violations of this policy by customers will be considered a material breach of their contract with CenturyLink and subject violators to legal action.

WAP in Customer Space

Customer may install wireless surveillance systems, including but not limited to Web cams, or Wireless Access Point (WAP) devices in your space or the CenturyLink data center.

Customer must comply with the following provisions:

- Customer shall provide CenturyLink with the SSID and MAC address of all access points deployed within the data center prior to installation
- Customer shall ensure that the location and placement of all devices relating to Customer's wireless network including, without limitation, wireless access points and associated network equipment including all parts thereto (collectively, "Devices") remain within the Customer Space;
- Customer acknowledges and agrees that unless otherwise agreed to in writing by the parties CenturyLink shall have no obligation to install or support the Devices, or to respond to any repairs, maintenance or distress calls regarding the Devices, and CenturyLink shall not be liable for any damage to or loss of the Devices absent CenturyLink's ' gross negligence or willful misconduct.
- Customer shall ensure that the Devices do not "block" or interfere with any wireless or other electronic signals;
- Upon Customer's receipt of written notice from CenturyLink that Customer's Device is blocking or causing interference with any of CenturyLink's or its customers' equipment, Customer shall immediately discontinue the use of any Device until such time as CenturyLink and Customer agree that such interference is resolved.
- Customer shall indemnify, defend and hold CenturyLink harmless from and against all third party claims, damages, liabilities, losses, and expenses, including reasonable attorneys' fees and expenses, arising out of or resulting from customer's use or placement of the Devices.

Shipping and Receiving Policy

Inbound Receiving: Generally, CenturyLink's Data Center Shipping and Receiving personnel are on-site during normal business hours. Regardless of whether your delivery is during normal hours or after hours, a service ticket generated by the customer in the SavvisStation portal or the CenturyLink Service Desk is required. If a package is delivered to the data center and a service request ticket is not opened by the Customer, CenturyLink data center personnel will open a service ticket on the Customer's behalf thus notifying the Customer that a delivery has been received.

All Customer equipment brought to the CenturyLink data center must enter the facility through the shipping and receiving area. Packages or equipment to be delivered to the data center **must** be addressed as follows:

"Your Company Name"
"Vantive Case Number for this Shipment"
"Your Customer ID"
"CenturyLink Contact Name"
c/o CenturyLink
CenturyLink Address

CenturyLink does not provide unlimited free storage. Items stored more than two business days may be

subject to storage charges. If equipment storage continues for more than thirty (30) days, CenturyLink may return, at Customer's expense, the stored customer equipment. Abandoned customer equipment will be considered stored equipment and will be subject to storage charges until it is removed from the data center by the customer. CenturyLink will not dispose of customer owned equipment.

Customer assumes any and all risk of loss or damage for any Customer equipment during the equipment storage period. If a data center physical address is unknown, please contact your Account Team or the CenturyLink Service Desk.

The Customer may arrange to have their equipment moved from the Shipping and Receiving area to their cage by opening a service ticket. No cardboard is permitted on raised floor and therefore all packaging materials will be discarded. CenturyLink Gold Support charges will be assessed to move customer equipment or packing materials from shipping and receiving to other areas of the data center.

Outbound Shipping: Upon request, CenturyLink will ship equipment on the customer's behalf. Customers are required to schedule the shipment with a carrier and for completing all necessary paperwork for the shipment. Customers are expected to provide appropriate containers and packing materials for the equipment to be shipped. As well, customers are required to pay for the shipping and insurance fees. CenturyLink will exercise due care in preparing the shipment requested by Customer, but will have no liability whatsoever in relation to the equipment or the shipping. CenturyLink Gold Support hours will be assessed for the time it takes to prepare and coordinate the shipment. Abandoned equipment will be returned to the customer. Customers will be invoiced for abandoned equipment storage and shipping fees.

All outbound shipment requests require a 48 hour advance notice via a ticket submission with the following information**:**

- The Customer's designated Shippers name
- The customer's shipping account number
- The Customer's billing address associated with the Shippers account number. CenturyLink will use this address as the return address for the package
- The "Ship To" address
- The declared value of the shipment
- Any special instructions regarding insurance, packing materials**,** shipment preparation, etc.
- Documentation required for the Shipment including packing slip/list, pro-forma order, etc.

Specific to the Las Vegas Data Centers

All shipments to the Las Vegas Data Centers are to be addressed as follows:

Attn: Your Company Name
Care of Switch
5335 W. Capovilla Ave

Las Vegas, NV 89118

This data center has specific times when they are able to receive deliveries. Shipping and receiving hours are between 9:00 AM and 4:00 PM Pacific Standard time. For any shipments that are delivered outside of this window to the Las Vegas data centers, Customer hereby agrees that it shall remit payment to CenturyLink for shipping and receiving fees of $250 per pallet received. Payments shall be made as invoiced by CenturyLink.

Shipments can be held for a maximum of 90 days from the date of delivery. Shipments stored in excess of 90 days will be assessed a monthly fee of $35 per square foot that the shipment occupies payable to CenturyLink.

Building Evacuation Policy

If the data center fire alarm or other life safety alarm is activated, customers must immediately evacuate the data center and report to an assembly point free and clear of danger. Evacuees are to remain at the assembly point until they are informed that they may leave the premises or enter the data center by Data Center Security, data center management, or the local authorities.

Parking Lot Policy

With the exception of multi-tenant facilities, parking is restricted to CenturyLink employees, customers, contractors, and visitors only. All other vehicles are subject to be towed at the vehicle owner's expense.

All vehicles must be parked in designated parking areas only. Vehicles parked outside designated parking areas are subject to be towed at the vehicle owner's expense. Customer or Visitor designated parking spaces are restricted for customer or visitor use only, respectively. Handicapped parking spaces are restricted to those vehicles displaying a current handicapped license plate or hanging placard issued by the respective State Department of Motor Vehicles. These spaces are designated with the International Symbol of Access (wheelchair symbol) or a blue curb.

Floor Tile Lifting Policy and Under Raised Floor Access

CenturyLink prohibits you from lifting data center floor tiles. Only CenturyLink employees may access and work below the raised floor area. If access is necessary during installation, you may request access via ticket. This may incur an additional fee. If you are already an installed customer, please contact the CenturyLink Service Desk. Floor tile pullers are not allowed in the data center or customer cages and will be confiscated accordingly. Access under the raised floor is strictly limited to authorized CenturyLink personnel. Adherence to this policy is strictly enforced and violators will be reported. Any breach of this policy is considered a material breach of customer's service agreement with CenturyLink and may be subject to termination.

Moving Heavy Equipment

Any customer equipment that is deemed too heavy to be moved by CenturyLink data center management

will be transported by a professional moving company and customer will be assessed appropriate charges for the move. Customers must take care to consider the weight of the equipment to be moved and consult with data center management to assure that no damage will be done to the data center flooring.

Specific to the Las Vegas Site

Switch personnel are responsible for moving all cabinets and oversized equipment within the facility. Customers may not move their cabinets to the T-SCIF. To schedule this please submit a ticket via the SavvisStation portal.

Specific to the Australia Sites

Racks are assembled and positioned by the personnel in the Australia sites. Customers may not detach, un-bay, disassemble or move cabinets or racks without prior written permission. Similarly, privacy panels between racks are not to be removed without prior written permission, even when you have contiguous racks.

All customer owned racks and cabinets will be assessed by data center personnel and implementation must be discussed and agreed with data center personnel prior to an order being placed.

Data Center Work Rules

CenturyLink Policy SV1-FAC-POL-MGT-1427

CenturyLink expects that anyone who enters the data center conduct themselves with the proper decorum and to honor all safety practices. It is vitally important that everyone understands the severe, negative impact that workers' actions can have on a site as a result of working inappropriately. These rules and guidelines have been developed to clarify CenturyLink's expectations and to reduce the chance of mistakes and unintended events. Failure to comply with any procedure will result in immediate removal from the site, may result in permanent loss of access to the facility, and possible loss of business for the company that the contractor represents.

In summary, the policy dictates that:

- The definition of a contractor is any person performing work in a CenturyLink data center that is not a CenturyLink employee or is not an authorized Customer representative performing work in the Customer Area.
- All contractors must be trained and display an understanding of the Data Center Work Rules. Contractors will adhere to the rules and guidelines set forth by the Facilities team at all times while on the premises.
- All contractors must pass a written exam demonstrating that they have read and understand the contents of this document. A passing score is 70%.
- Contractors who complete orientation and pass the written exam will receive a certification good for one year from the completion date.
- Upon expiration of certification the contractor will be asked to review the Data Center Work Rules

making note of any changes in policy and take another written exam.

It is the responsibility of the CenturyLink Project Manager to ensure that all contractors are aware of, understand, and have been trained on the Data Center Work Rules and requirements.

Failure to know or comply with the policy is grounds for immediate removal from the site, perhaps permanently. All personnel allowed access to critical areas must review these Work Rules and demonstrate their knowledge of the Rules most applicable to their activity on site at least every twelve months.

Work Rules Specific to the Australia Data Centers

Permit to Work

Anyone who will be performing the below specified types of work at a facility will require an approved Permit to Work (PTW) application priori to commencing the potentially hazardous work. The Permit to Work must be submitted to be approved at least seven days prior to the planned commencement of work.

This includes:

- Dust-producing work
- Hot work
- Electrical work
- Confined-space work
- Cabling installation or related work, external to a rack
- Planned preventative maintenance

The Permit to Work application can be submitted through the First Touch Response Center.

All contractors are to be appropriately licensed, insured and qualified for the work they are undertaking. Documents required to be attached to each Permit to Work form include:

- Proof of current insurances
- JSA/SWMS (Job Safety Analysis/Safe Work Method Statement)s

Crash Carts and Tools

Crash carts (mobile units housing a keyboard, monitor and mouse) and tools are provided on a limited basis as a courtesy to our customers. They are provided on a first-come, first-served basis. Crash carts are required to be signed out with the onsite CenturyLink data center personnel and returned within a 24-hour window. As crash carts may not always be available, it is encouraged that workers to come prepared to conduct their intended work.

Telephone Use in the Data Center

The red and black phones in the data center are used for emergencies only. CenturyLink encourages customers to install a Plain Old Telephone System (POTS) telephone line in your space, or to bring cellular phones to use while working within the data center.

Conference Rooms

Customer is permitted to reserve available data center conference and team rooms on a first come, first serve basis. Customer must request a room at least 24 hours in advance and via service ticket. Customer's use of these rooms is limited to one (1) day a week. Notwithstanding anything to the contrary, Customer's use or occupancy of the room shall not exceed five (5) days in any given month. Conference and team rooms are available during normal business hours, at the sole discretion of the data center management. Customers are to return the conference room to the condition in which it was received. The room shall be left free of meeting materials and food items.

Data Center Safety and Environmental Policy

In order to provide a safe and secure service, CenturyLink requires that all customers adhere to the following guidelines:

- **Zero Tolerance Policy:** Customers must keep their areas clean at all times. Cages must be free of debris. Cardboard boxes are strictly prohibited. Due to fire, safety, and environmental requirements, this policy is strictly enforced and CenturyLink reserves the right, in its sole discretion and with Customer's approval which is hereby granted, to immediately remove any cardboard, paper, debris etc. from any and all customer cages. CenturyLink will use reasonable efforts to notify the customer of such non-compliance after removal. In the event CenturyLink removes such items, there will be a Gold Support charge billed to Customer's account and Customer acknowledges and agrees to render payments for such Service at the Gold Support hourly rate as invoiced by CenturyLink.

- Customers may not store combustible materials or paper products (including cardboard and boxes) anywhere in the data center. Unused cabling must be stored out of sight and equipment stored without impeding airflow. Cabling may not be draped in aisle ways or hinder clearance around cabinets.

  Customers must keep tile vents clear of any obstruction. Non-functioning equipment and miscellaneous items must be stored out of sight and organized inside the Customer's cage at the end of each working day.

Prohibited Materials in CenturyLink Data Centers

The following items are prohibited in CenturyLink data centers:

- Food or drink – prohibited on the raised floor
- Tobacco products (including smokeless) – prohibited on the raised floor

- Explosives, firearms or weapons of any type (See Weapons Section for further details)
- Hazardous materials or other chemicals
- Alcohol, illegal drugs, as well as other intoxicants
- Magnets and electromagnetic devices
- Radioactive materials
- Photography equipment (unless preauthorized by data center Management) or recording equipment of any kind (other than tape backup equipment)

- UPS equipment, other than what is provided by CenturyLink, is strictly prohibited.
- Paper products (other than equipment manuals) or other combustible materials of any kind, including cardboard and boxes

Weapons

CenturyLink strictly prohibits firearms or other form of weapons, including but not limited to knives (other than small pocket knives), explosives (including fireworks), chemicals or other substances, and/or hazardous devices in its data centers.

Employees, contractors, customers and visitors are required to lock weapons safely in their personal vehicle whenever the vehicle is on CenturyLink property. When locking weapons in a personal vehicle, the weapon is expected to not have ammunition in it, and the ammunition stored in a separate part of the vehicle. Weapons are not to be removed from the vehicle while the vehicle is on CenturyLink property and should be out of visibility of others if possible. Further requirements for handling and storing weapons differ by location and are governed by state and local laws.

Bolt down, Seismic Bracing & Grounding of Cabinets and Racks

Location-specific seismic compliance is required at our CenturyLink data centers and dictated by local building code and NEBS GR-63-CORE certification. Structural bracing systems and customer provided cabinets must meet or exceed seismic design requirements of local building codes for lateral seismic design. CenturyLink customers are responsible for all costs associated with seismic bracing of cabinets and racks.

For the safety of customers and data center employees, all cabinets and racks in all data centers must be anchored, braced and grounded in accordance with the requirements of the 2012 International Building Code and the National Electric Code. All customer-owned cabinets will be installed **only** by CenturyLink personnel.

Compliance Audit Reporting

CenturyLink performs periodic audits of its data centers, which result in the issuance of audit reports or certificates. Customers may request copies of these reports through their account team or via the Service Desk after signing CenturyLink's Non-Disclosure Agreement specific to the disclosure of audit

documentation.

Available reports include SSAE 15 SOC 1, SOC2, PCI DSS, ISO 27001, SafeHarbor, Global Risk Management, Business Continuity and Disaster Recover (BCDR), HIPPA and FISMA (NIST 800-53) and SOC 1 Type II (SSAE 16/ISAE 3402). The ISO 27001 Certificate is applicable to UK, Germany, Singapore, and Tokyo data centers only. The availability of reports may change from time to time as determined by CenturyLink in its sole discretion.

Customers may request additional audit information via service ticket and subject to an additional charge at the Gold Support rate. Depending on the request, Customer may be required to enter into an amended NDA to cover additional information.

Customer Cabling

Cabling within customer cages must be installed in an appropriate industry standard discipline and professional manner. This requires that the customer purchase cabling services from CenturyLink or be assessed a compliance and oversight fee that will be charged to the customer in the form of Gold Support. Prior to CenturyLink granting Customer's third party cabling vendor ("Cabling Vendor") permission to perform cabling installation within a CenturyLink data center, the Cabling Vendor's foreman must pass the CenturyLink Facilities Work Rules test and the Structured Cabling Contractor Exam with a score of at least 80%. In accordance with CenturyLink's cabling standards, Customer shall be responsible for the payment of a compliance and oversight fee ("Compliance and Oversight Fee") which will be charged to Customer in the form of Gold Support hours throughout the duration of the Cabling Vendor's provisioning of structured cabling. The Compliance and Oversight Fee will appear on the Customer invoice as Gold Support.

Cabling must be properly run and secured within cabinets, by using overhead and vertical cable management devices. Cabling must be installed in a safe manner so that it in no way impedes aisles, floor, and entranceways or presents a fire hazard.

CenturyLink's standard cable management will be represented within the "T-Series Layer1 Documentation set". Cable management is defined as (1) overhead and/or under floor support such as basket tray, ladder rack, fiber guide and the associated support material, (2) the vertical and horizontal support panels designed and installed to accompany rack and cabinet configurations, and (3) routing of patch cords or interconnect cabling (copper and fiber) within the racks and cabinets between connectivity panels (patch panels) and/or active equipment All other wire management equipment will incur an additional fee. All cabling must be plenum rated and meet the UL minimum code standards and the National Electrical Code NFPA-70. CenturyLink recommends clear labeling at each end of all installed cables. CenturyLink reserves the right to remove any non-compliant cabling after the notification of a cabling violation per the notification process that is outlined in the CenturyLink Schedule.

Billing Inquiries

Billing inquiries can be made by e-mail at billingdepartement@centurylink.com Up-to-date contact information can always be found on your invoice. You can also contact the alias above (Billing Support team) for copies of billing invoices.

SLA Credit Requests

If you feel you are entitled to a credit, as per your Service Level Agreement, please timely submit your request to billingdepartment@centurylink.com. Include in your e-mail any trouble ticket/case information; dates, and other specifics that you feel will be useful in evaluating your request.

Key Contacts

Dedicated Colocation Support Team

Self Service Portal: www.savvisstation.com

Email: Colo.Support@centurylink.com

Phone: 800-884-3082

Client Response Center

North America: 888-638-6771

EMEA: 00800 8288 4743

Asia Pacific: +65 63058099

Request@centurylink.com

incident@centurylink.com

Billing
Phone: 1-877-SAVVIS-7, Option 2
E-mail: billingdepartment@centurylink.com